Digitalpolitik

Eine Einführung

Eine Publikation initiiert von Wikimedia Deutschland und iRights.international, mit Unterstützung von ICANN

Herausgeber: Lorena Jaume-Palasí, Julia Pohle, Matthias Spielkamp







Vorwort

Warum Digitalpolitik?

Nie zuvor hat eine Entwicklung die Welt so schnell und so grenzüberschreitend verändert wie die Digitalisierung und die Verbreitung des Internets. Das stellt unsere Gesellschaften vor enorme Herausforderungen. Wie können wir gestalten, was derart schnell voranschreitet und einen massiven Einfluss auf unser gesamtes Leben ausübt – auf unsere Art zu kommunizieren, zu arbeiten und zu lernen, zu entspannen und zu spielen, ja selbst zu lieben und zu sterben?

Wir müssen in diesem Reader *Digitalpolitik. Eine Einführung* nicht mehr deutlich machen, dass alle Lebensbereiche eine digitale Dimension haben. Das Ziel dieser Publikation, die von Wikimedia Deutschland und iRights.international initiiert und von ICANN unterstützt wurde, ist vielmehr zu erläutern, wie sich Digitalisierung und Politik gegenseitig beeinflussen. Die Wechselwirkung von Digitalisierung und Politik wird im Englischen als Internet Governance bezeichnet. In Deutschland setzt sich für das gleiche Phänomen zunehmend der Begriff Digitalpolitik durch.

Tatsächlich gibt es in der deutschen Sprache keinen guten Begriff für das, was im Englischen „Governance" genannt wird. Es ist weder Regierungs- noch Staatsführung, denn es geht um mehr als die Regierung, und das Konzept *Führung* setzt in unserem Verständnis voraus, dass ein Einzelner die Richtung vorgibt – selbst wenn damit eine einzelne Regierung gemeint ist. Ähnliches gilt für Steuerung und Lenkung. Am nächsten kommt man der Idee sicherlich mit den Begriffen des Aushandelns und der Koordination. Man mag einwenden, dass das schon immer die Aufgabe der Politik war: Prozesse zu koordinieren und Kompromisse auszuhandeln zwischen den Interessen von Bürgerinnen und Bürger und denen von Unternehmen, zwischen Anhängern und Anhängerinnen der einen und der anderen Partei.

Dennoch ist der Aushandlungs- und Koordinationsprozess, der sich in der globalen Digitalpolitik entwickelt hat, ein anderer. Es sind dabei andere Stakeholder an Bord, andere Akteure also, die sich am Aushandlungsprozess beteiligen und dort ihre Stakes, das heißt ihre Interessen vertreten. Die Reihe der beteiligten Stakeholder erstreckt sich von nationalen wie internationalen Standardisierungsgremien über globale Internetunternehmen und über Organisationen wie ICANN, die die Domainnamen des Internets verwalten, bis hin zu lokalen Nichtregierungsorganisationen, Staaten

und einzelnen Aktivisten. Darum ist von so genannten Multistakeholder-Prozessen die Rede.

Es sind aber nicht nur andere Akteure, die die Gestaltung des Internets als einer Art 'Betriebssystem der Gesellschaft' aushandeln. Sie tun das auch in anderen Foren als bisher. Zu diesen Foren zählen etwa das globale Internet Governance Forum (IGF), regionale und nationale IGFs, die Freedom Online Coalition und die Konferenzen der Internet Society oder die auf einem informellen Zusammenschluss basierende Manila-Gruppe, in der Organisationen und Individuen Prinzipien zur Haftung für Intermediäre entwickeln.

Das soll nicht bedeuten, dass 'die Politik', bestehend aus Regierungen und Parlamenten als Repräsentanten der Bürgerinnen und Bürger eines Landes (oder einer Gemeinschaft wie der EU), weniger relevant würden. Es geht vielmehr darum zu sagen, dass diese Politik sich in den Dialog begeben muss mit den neuen Akteurinnen und Akteuren, in neuen Foren, mit neuen Prozessen. Die gegenseitige Beeinflussung nationaler und europäischer, europäischer und globaler, globaler und nationaler Digitalpolitik ist nicht nur ein Faktum, sondern vor allem eine Chance. Erstmals wird es möglich, tatsächlich alle Interessengruppen, die von einem Handlungsfeld oder einem politischen Problem betroffen sind, als gleichberechtigte Beteiligte in den politischen Dialog und Verständigungsprozess einzubeziehen. In diesem Prozess erfolgt eine echte nicht-hierarchische Regelfindung durch alle Beteiligten. Resultat dieser Multistakeholder-Prozesse sind meist Verständigungspapiere, die nur empfehlenden Charakter haben, aber idealerweise von einer großen Mehrheit akzeptiert und respektiert werden.

Selbstverständlich gibt es in diesen Prozessen Machtungleichgewichte, massives Lobbying durch Unternehmen, Hinterzimmer-Deals zwischen Regierungen oder bisweilen unfaire Anprangerungen durch 'Pressure Groups'. Das Einbeziehen unterschiedlicher Akteursgruppen in einen koordinierenden Dialog ist kein idealer Weg einer verständigungsorientierten Aushandlung, die nur auf dem „zwanglosen Zwang des besseren Argumentes" beruht. Aber es ist eine neue Stufe deliberativer Politik, die den Gestaltungsanforderungen einer vernetzten Welt angemessen ist.

Diese Möglichkeit richtig zu verstehen und zu nutzen, und damit größtmögliche Akzeptanz für die Ergebnisse herbeizuführen, macht Digitalpolitik aus.

Lorena Jaume-Palasí Julia Pohle Matthias Spielkamp

Inhaltsverzeichnis



Einführung in die Digitalpolitik

Ob in der Debatte um Fake News und Hate Speech, ob im Zuge des NSA-Überwachungsskandals oder mit Blick auf Datenschutz und Privatsphäre in sozialen Netzwerken: Digitalpolitik ist in den vergangenen Jahren immer stärker ins Blickfeld der Öffentlichkeit gerückt. Auch in der Politik nimmt die Regulierung im Internet als globalem Politik- und Wirtschaftsraum einen immer höheren Stellenwert ein – auf nationaler und internationaler Ebene.

JULIA POHLE, LORENA JAUME-PALASÍ, MATTHIAS SPIELKAMP

Die immer breitere Aufmerksamkeit macht klar: Heute haben fast alle politischen Themen eine digitale Dimension. Von Gesundheit und Verkehr über Presse und Öffentlichkeit, Urheberrecht und Sicherheit bis zu Arbeit, Grundrechten, Wirtschaft und Finanzen – nahezu sämtliche Bereiche sind von der stetig zunehmenden Digitalisierung der Gesellschaft betroffen.

Angesichts dieser Veränderungen müssen Gesetze und Regulierungskompetenzen auf nationaler und europäischer Ebene angepasst werden.

Doch die politischen Argumente und Agenden des digitalisierten Zeitalters werden in vielen Fällen in Foren abseits der Bundestags- und Kabinettsdebatten ausgetauscht und geschmiedet. So entscheiden Standardisierungsgremien auf internationaler Ebene über die technische Gestaltung von Dienstleistungen und Prozessen weltweit, die dann sowohl in der Wirtschaft als auch in Politik und Verwaltung eingesetzt werden. In internationalen Debatten, zum Beispiel innerhalb der Vereinten Nationen (VN), verständigen sich Stakeholdergruppen aus Politik, Wirtschaft, Zivilgesellschaft, Wissenschaft und technischer Community auf Best Practices, die ebenfalls oftmals in nationale Gesetzgebung einfließen. Mit Blick auf die digitale Dimension politischer Themenfelder findet somit eine Verschiebung der Strukturen statt, in denen politischen Entscheidungen getroffen und Meinungen durchgesetzt werden: Digitalpolitik hat eine eigene Akteurs- und Forenlandschaft, die bisher zumeist nur einer kleinen Fachöffentlichkeit präsent ist.

Entscheiderinnen und Entscheider in Deutschland, die sich mit digitalpolitischen Problemen beschäftigen, müssen diese Akteure und Gremien kennen und verstehen, wollen sie neue Themen, Risiken und Chancen erkennen, ihre Strategien effektiver gestalten und Prozesse der Meinungs- und Entscheidungsbildung prägen. Der Reader *Digitalpolitik. Eine Einführung* stellt verständlich und praxisorientiert eine Auswahl von Themen vor, die im Fokus digitalpolitischer Debatten stehen, und erläutert, wer sie vorantreibt und wie man sie mitgestalten kann. Es handelt sich dabei um ausgewählte Querschnittsthemen, die trotz ihrer Spezifität in etliche zentrale Politikbereiche hineinreichen und deren Themenspektrum beeinflussen.

Politische Argumente und Agenden werden in Foren abseits von Bundestag und Kabinett ausgetauscht und geschmiedet.

Von der Digitalpolitik zur Internet Governance

Wie fast alle Politikbereiche wird auch Digitalpolitik heutzutage sowohl auf europäisch-nationaler als auch auf globaler Ebene diskutiert und gestaltet. Auf den ersten Blick scheinen sich die beiden Ebenen mit unterschiedlichen Aspekten der Nutzung und Weiterentwicklung des Digitalen und den dazugehörigen Infrastrukturen zu beschäftigen: Im national-europäischen Kontext spielen auf den ersten Blick vor allem gesellschaftliche und

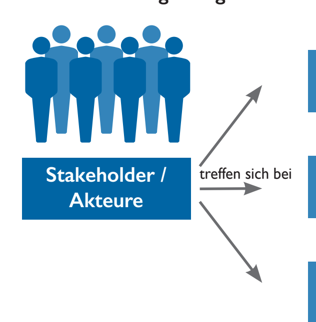
Akteure und Handlungsfelder: Deutschland

Bereits auf nationaler Ebene müssen sich viele verschiedene Akteure über die digitale Dimension politischer Probleme einig werden. So besitzt Deutschland kein einzelnes Ministerium mit Regulierungskompetenz für Digitalpolitik. Stattdessen hat die Bundesregierung 2014 ein Strategiepapier für die Digitalisierung beschlossen, die sogenannte Digitale Agenda. Diese skizziert grob die Vorhaben der deutschen Digitalpolitik und überträgt die Federführung drei Ministerien gleichzeitig: dem Bundesministerium für Wirtschaft und Energie (BMWi), dem Bundesministerium des Innern (BMI) und dem Bundesministerium für Verkehr und digitale Infrastruktur (BMVI). Diese drei haben gemeinsam die Aufgabe, die einzelnen Maßnahmen der deutschen Digitalpolitik zu koordinieren, die in den sieben Kapiteln der Digitalen Agenda zusammengefasst sind, und erklärtermaßen alle Aspekte des digitalen Wandels in Deutschland abdecken. Dazu widmen sich die Handlungsfelder der Digitalen Agenda unter anderem dem Breitband-Ausbau, der Zukunft von Wirtschaft und Arbeit in einer immer stärker digitalisierten Welt, der Sicherheit der Nutzerinnen und Nutzer im Internet, aber auch dem digitalen Wandel in der Wissenschaft oder der Bedeutung von Digitalpolitik in den internationalen Beziehungen.

Die Zuständigkeiten für digitalpolitische Aspekte sind jedoch nicht allein auf die drei federführenden Ministerien beschränkt. So bringen neben Wirtschafts-, Innen- und Verkehrsressort auch weitere Ministerien ihre Initiativen ein – das Arbeitsministerium etwa zum Thema Digitale Arbeit oder das Forschungsministerium zur Gründung eines Internet-Forschungsinstituts. Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) widmet sich unter anderem der Regulierung der digitalen Dimension von Strafverfolgung, Urheberrecht und Verbraucherschutz. Das Finanzministerium richtet einen Rat zu Finanztechnologien ein und beschäftigt sich unter anderem mit Blockchain-Technologien, so wie auch das Entwicklungshilfeministerium mit Blick auf den Globalen Süden. Und im Auswärtigen Amt und dem Verteidigungsministerium wurden über die Jahre Regulierungskompetenzen für internetpolitische Fragen angesiedelt, zum Beispiel für Cybersicherheit.

wirtschaftliche Veränderungen durch die Digitalisierung eine Rolle, etwa die Vernetzung von Alltagsgegenständen über das Internet der Dinge (in Deutschland auch unter „Industrie 4.0“ thematisiert), die Sicherheit elektronischer Kommunikation sowie die Gewährleistung von Meinungs- und Pressefreiheit im Netz oder die Regulierung von Intermediären (beispielsweise Social-Media-Plattformen). Durch Deutschlands Einbindung in die Europäische Union (EU) ist zudem die Regelsetzung durch die EU-Ebene von großer Bedeutung. Kontroversen wie jüngst um die Datenschutzgrundverordnung oder die Richtlinie zu Netzneutralität werden dadurch Teil der gesellschaftlichen und politischen Diskussion in Deutschland. Die globale Ebene hingegen, so die häufige Ansicht, widme sich vergleichsweise abstrakten und unpolitischen Themen wie technischen Stan-

Wissenschaft Zivilgesellschaft
Unternehmen Regierungen



Stakeholder / Akteure

treffen sich bei

globales UN Internet Governance Forum (IGF)

regionale IGF und andere Multistakeholder-Foren

nationale IGF und andere Multistakeholder-Foren

erzeugen

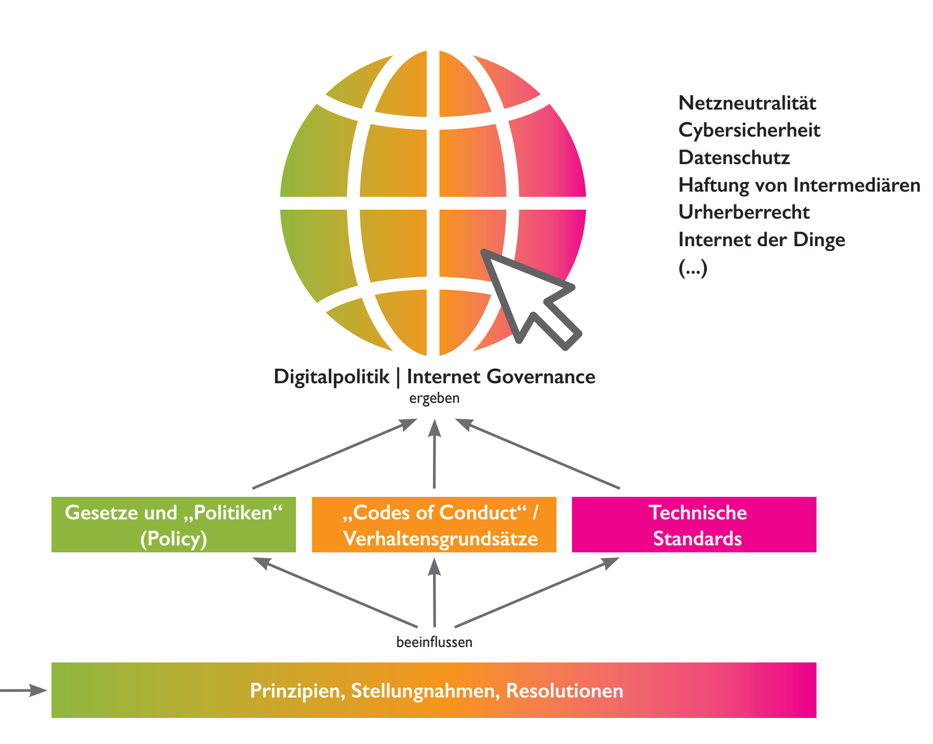


offene Diskussionen

daraus folgen

dards, der Vergabe von IP-Adressen oder der Organisation von Domain-Endungen wie .com und .net – ein Aufgabenfeld, das meist mit dem englischen Begriff Internet Governance bezeichnet wird. Zwar spielen auch in diesen Regulierungsbereichen Staaten wie Deutschland eine Rolle. Die Entscheidungsgremien sind jedoch andere und ihre Themen prägen nicht so sehr die gesellschaftliche Diskussion und politische Regelsetzung in Deutschland. Deshalb entsteht der Eindruck, dass es sich bei national-europäischer Digitalpolitik und globaler Internet Governance um zwei Paar Schuhe handele.

Diese Publikation soll deutlich machen: Die Vorstellung einer inhaltlichen Trennung national-europäischer Digitalpolitik von globaler Internet Governance ist nicht nur falsch – sie ist mit Blick auf die zukünftige Regulierung und Entwicklung des Internets auch sehr kurzsichtig. Denn die in den



Internet-Governance als Multistakeholder-Prozess
(eigene Darstellung)

Akteure und Handlungsfelder: Europa

Die digitalpolitische Arbeit Deutschlands wird stark von der Europäischen Union beeinflusst, deren Entschlüsse und Richtlinien in geltendes nationales Recht umgesetzt werden müssen. Die EU-Kommission hat bereits 2010 eine Europäische Digitale Agenda verabschiedet – als eine der sieben Säulen der Strategie Europa 2020, die einen bunten Strauß verschiedener Handlungsfelder der Kommission umfasst. Ein wichtiger Bestandteil der Europäischen Digitalen Agenda ist der Digitale Binnenmarkt. Den freien Handel, der „offline" im gemeinsamen Markt der EU-Mitgliedsstaaten bereits seit Jahrzehnten für wirtschaftlichen Wohlstand sorgt, soll der Digitale Binnenmarkt auch „online" verwirklichen. Weitere Bereiche der europäischen Agenda sind etwa sind schnelleres Internet für Unionsbürgerinnen und -bürger sowie ein reformiertes Urheberrecht. Doch auf EU-Ebene sind die Kompetenzen für Digitalpolitik stark verteilt: Verantwortlich für den Digitalen Binnenmarkt ist innerhalb der EU-Kommission die Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG Connect). Um den Datenschutz kümmert sich dagegen die Generaldirektion Justiz und Verbraucher (DG Justice). In Zusammenarbeit mit der Kommission sind auf EU-Ebene weitere Institutionen im Bereich Digitalpolitik aktiv, vor allem das Europäische Parlament und der Ministerrat der Europäischen Union, die als Gesetzgebungsorgane entscheiden.

Weitere wichtige Akteure sind das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation BEREC, das im September 2016 das Prinzip der Netzneutralität festgeschrieben hat, sowie der Europäische Datenschutzbeauftragte, der die Kommission in Datenschutzfragen berät und die Kooperation zwischen nationalen Datenschutzbehörden unterstützt. Nicht zuletzt übt der Europäische Gerichtshof (EuGH) Einfluss auf die Digitalpolitik aus – indem er Streitfälle im Bereich der Richtlinien und Verordnungen letztinstanzlich entscheidet. Neben den öffentlichen Akteuren wie Rat, Parlament und Kommission mischen in Brüssel aber auch zahlreiche private Organisationen aus Wirtschaft und Zivilgesellschaft in der EU-Politik mit, deren Einfluss nicht unterschätzt werden darf. Weitere europäische Akteure und Gesetzestexte jenseits der Europäischen Union haben oft direkten Einfluss auf die deutsche Gesetzgebung, wie zum Beispiel die Konvention 108 des Europarates oder der Europäische Gerichtshof für Menschenrechte (siehe dazu den Beitrag von Lorena Jaume-Palasí zum Thema Datenschutz).

nationalen und globalen Gremien diskutierten Fragestellungen unterscheiden sich nur auf den ersten Blick. Tatsächlich handelt es sich um die gleichen technischen, wirtschaftlichen und gesellschaftspolitischen Fragen, diskutiert in verschiedenen Settings und unter Einbeziehung unterschiedlicher Akteure. Nicht selten werden auf einer Ebene Reformvorhaben angestoßen, die auf einer anderen Ebene nicht verfolgt oder nicht sinnvoll umgesetzt werden können. Ein Beispiel dafür führt Hauke Gierow in seinem Beitrag zum Thema Breitbandausbau vor. Das „Recht auf einen Internetzugang" wurde auf globaler Ebene beschlossen und kodifiziert. Die technische Umsetzung der Versorgung mit Internetzugang obliegt nationalen Bemühungen, privaten Vereinen und Unternehmen. Über das „Wie" der Umsetzung (zum Beispiel durch Angebote des „Zero-Rating") wiederum wird ein globaler politischer Diskurs geführt.

Ein anderes Beispiel für das Zusammenspiel von nationaler, europäischer und globaler Digitalpolitik ist das Thema Netzneutralität. Zwar nimmt die EU-weite Regelung von Netzneutralität ausdrücklich Bezug auf die Sicherung der Meinungsvielfalt und das Recht auf freie Meinungsäußerung. EU-Politik allein jedoch ist nur ein Teil des Puzzles, um Probleme, die in Bezug auf Netzneutralität diskutiert werden, zu beheben. Meinungsvielfalt und die Gewährleistung einer Infrastruktur für öffentliche Kommunikation sind ebenso bedroht durch Zersplitterung und „Applicancization" wie durch Nicht-Neutralität in der Datenübermittlung (siehe dazu den Beitrag von Grötker/Greis). Medienpolitische Strategien, die hier eigentlich notwendig wären, sind allerdings auf EU-Ebene kaum möglich. Globale Vereinbarungen könnten hier helfen. Beispiele dafür sind verschiedene Initiativen, um global agierende Plattformen zu regulieren. Davon handeln die Beiträge von Joerg Heidrich und Matthias C. Kettemann zum Thema Intermediäre. Martin Schallbruch und Isabel Skierka verdeutlichen in

ihren Beiträgen zur Cybersicherheit, wie nationale Bemühungen um Cybersicherheit und IT-Sicherheit eingebunden sind in europäische Richtlinien und die Budapest Convention des Europarates auf der einen Seite und in globale Vereinbarungen im Rahmen der Vereinten Nationen auf der anderen Seite. Hinzu kommen, auf informeller Ebene, als internationale Netzwerke organisierte digitale Notfallteams für Organisationen oder ganze Länder, sogenannte Computer Security Incident Response Teams (CSIRTs).

Der Multistakeholder-Ansatz

Digitalpolitik auf national-europäischer und globaler Ebene unterscheidet sich also nicht primär durch gänzlich verschiedene Problem- und Handlungsfelder. Vielmehr sind die Unterschiede bei den beteiligten Akteuren zu suchen, bei den Prozessen, aber auch bei den Regulierungspraktiken und der Verbindlichkeit der Rechtsmittel. Auf nationaler und EU-Ebene wird Regulierung zumeist durch eine übergeordnete Autorität festgelegt und resultiert in verbindlichen Regeln und Gesetzen. Globale Prozesse laufen dagegen dezentral ab. Statt einer übergeordneten Strategie oder eines koordinierten Gesetzgebungverfahrens kommen Abstimmungen in zahlreichen parallel laufenden, voneinander unabhängigen oder sich nur marginal überschneidenden Prozessen zustande. Das Besondere an der globalen Digitalpolitik ist zudem, dass sie nicht hauptsächlich von Politikern gemacht wird. Seit der Entstehung des Internets als globales Netzwerk sind in internationalen Gremien eine Vielzahl unterschiedlicher Akteure und Interessengruppen involviert.

Resultat dieser Multistakeholder-Prozesse sind meist Verständigungspapiere, die nur empfehlenden Charakter haben, aber idealerweise von einer großen Mehrheit akzeptiert und respektiert werden.

Der Modus der Verhandlung und Beschlussfassung, wie er sich in diesen globalen, dezentral ablaufenden Prozessen etabliert hat, ist für sich genommen einer Betrachtung wert. Bei diesem sogenannten Multistakeholder-Ansatz (bisweilen auch Multi-Akteurs-Ansatz genannt) geht es darum, alle Interessengruppen, die von einem Handlungsfeld oder einem politischen Problem betroffen sind, als gleichberechtigte Beteiligte in den politischen Dialog und Verständigungsprozess einzubeziehen. Hier dominiert somit im Gegensatz zur nationalen Politik eine nicht hierarchische Regelfindung durch alle Beteiligten. Auf die egalitäre Repräsentanz der verschiedenen Gruppen hingegen wird – anders als sonst in der Politik – weniger geachtet. Resultat dieser Multistakeholder-Prozesse sind – mit einigen Ausnahmen – meist Verständigungspapiere, die nur empfehlenden Charakter haben, aber idealerweise von einer großen Mehrheit akzeptiert und respektiert

werden. Das Verfahren wird seit Jahren in Organisationen wie ICANN oder bei globalen Events wie dem IGF und der NetMundial-Konferenz mal mehr, mal weniger erfolgreich angewendet. In der deutschen Digitalpolitik sind Multistakeholder-Prozesse dagegen bisher nur in Ansätzen zu finden. Beispiele sind die Enquete-Kommission Internet und digitale Gesellschaft (2010 - 2013), die Ausarbeitung eines Positionspapiers zur letzten ICANN-Reform 2015 oder das seit 2008 jährlich stattfindende Internet Governance Forum Deutschland (IGF-D).

Technologien verändern mit zunehmender Geschwindigkeit unsere Gesellschaften und die Rahmenbedingungen unserer Politik. Neue Akteure, Prozesse und Regulierungspraktiken bilden sich aus: Die Herausforderungen internationaler Internet Governance für die deutsche Digitalpolitik sind vielfältig. Entsprechend groß sind aber auch die Chancen. Wer sie nutzen will, muss diese Akteure und die Foren, in denen die neuen Prozesse und Regulierungspraktiken stattfinden, ebenso kennen wie die Wirkung, die sie auf die deutsche Digitalpolitik und im Zusammenspiel mit ihr entfalten. Der vorliegende Reader bietet eine Übersicht, die an der politischen Praxis orientiert und auf sie ausgerichtet ist. Er soll damit nicht mehr – aber auch nicht weniger – sein als ein Startpunkt und Leitfaden für Entscheidungsträgerinnen und Entscheider, die diese Entwicklungen nicht nur verstehen, sondern gestalten wollen. ■

Akteure und Handlungsfelder: Global

Neben der europäischen Digitalpolitik haben auch etliche global erfolgende Abstimmungen und Prozesse Einfluss auf Internetregulierung in Deutschland. So werden Lösungen für viele digitalpolitische Probleme in internationalen Standardisierungsgremien geprägt und durchgesetzt. Diese Gremien haben unter anderem starke Auswirkungen auf politische Bereiche, die sich mit Content, also Inhalten im Netz, befassen, sei es Presse- und Äußerungsrecht, Datenschutz oder Cybersicherheit. Der Einfluss von internationalen Institutionen wie der Weltorganisation für geistiges Eigentum (WIPO), aber auch von Selbstregulierungspraktiken wie Creative Commons (siehe dazu den Beitrag von Paul Klimpel) ist allen involvierten Akteuren gut bekannt. Weniger im Fokus stehen dagegen internationale Gremien wie die Internet Engineering Taskforce (IETF) oder das Institute of Electrical and Electronics Engineers (IEEE), die durch Standardsetzung (insbesondere mit bestimmten Algorithmen und Diensten wie E-Mail, Datei-Übertragungen und Verschlüsselung) dem Internet überhaupt erst zur weltweiten Verbreitung verholfen haben. Ein anderes Beispiel sind Standardisierungsinstitutionen wie die ISO (International Organization for Standardization), die im Bereich Automatisierung maßgeblich die Entwicklung von Robotern aus einer praxisorientierten Perspektive heraus regelt (siehe dazu den Beitrag von Jürgen Geuter zum Internet der Dinge sowie Lorena Jaume-Palasís und Matthias Spielkamps Auseinandersetzung mit Big Data und Algorithmen). Aber auch die Koordinierung und Verwaltung von Internet-Adressen wie bundestag.de, twitter.com und wikipedia.org mittels des sogenannten Domain Name System (DNS) gehört zur internationalen Regulierung des Internets, ausgeführt durch eine der prominentesten Internet-Organisationen weltweit, die Internet Corporation for Assigned Names and Numbers (ICANN).

Die Aushandlung internationaler Abkommen und die Abstimmung über Codes of Conducts und Minimalstandards, die zwischen unterschiedlichen Regeln und Standards vermitteln, geschieht ebenfalls im Rahmen von globalen Prozessen. Teilweise werden diese durch internationale Organisationen ausgerichtet. So hat die Internationale Fernmeldeunion (ITU) bereits in den Jahren 2003 und 2005 die bisher größte globale Konferenz zu digitalpolitischen Themen veranstaltet, den sogenannten Weltgipfel zur Informationsgesellschaft (World Summit on the Information Society, WSIS). Zum anderen bieten sich Gelegenheiten zum internationalen Austausch bei einer Vielzahl von regelmäßigen Foren, wie dem seit 2006 jährlich von den Vereinten Nationen organisierten Internet Governance Forum (IGF) oder bei einmaligen Treffen wie der NetMundial-Konferenz, die 2014 in São Paulo unter brasilianischer Schirmherrschaft stattfand. Letztere hatte zum Ziel, einen globalen Konsens zu Prinzipien und Normen von Internetregulierung zu finden, unter Beteiligung einer großen Anzahl von Stakeholdern aus Politik, Wirtschaft, technischer Community, Wissenschaft und Zivilgesellschaft.



NSA-Skandal nur Spitze des Eisbergs

Mit der Veröffentlichung der NSA-Dokumente und dem Cyberangriff auf den Deutschen Bundestag hat Cybersicherheit eine neue sicherheitspolitische Dimension erhalten.

MARTIN SCHALLBRUCH

Stellenwert der Diskussion über Cybersicherheit

Die politische Diskussion über Cybersicherheit in Deutschland wurde in den vergangenen Jahren maßgeblich durch zwei Ereignisse motiviert: die Veröffentlichung der NSA-Dokumente durch Edward Snowden im Jahr 2013 und den Cyberangriff auf den Deutschen Bundestag im Jahr 2015. Damit hat die deutsche Debatte über Cybersicherheit erstmals eine sicherheitspolitische Dimension erhalten, die über die Abwehr von Cybercrime und den Schutz von Infrastrukturen gegen Ausfälle hinausgeht. Mittlerweile ist Cybersicherheit unter Sicherheitspolitikern in Bund und Ländern eines der am meisten diskutierten Themen. Die deutsche Öffentlichkeit hat sich

intensiv mit den Enthüllungen von Edward Snowden und den Fähigkeiten der NSA zum Eindringen in IT-Systeme beschäftigt. Einen Höhepunkt erlebte die Debatte im Herbst 2013, als bekannt wurde, dass die NSA über Jahre das Mobiltelefon von Bundeskanzlerin Merkel abgehört hat. Das zeitliche Zusammenfallen dieses Ereignisses und der NSA-Enthüllungen mit der Bildung der Großen Koalition Ende 2013 führte dazu, dass der Koalitionsvertrag von CDU/CSU und SPD Fragen der IT- und Cybersicherheit in einem nie zuvor gesehenen Ausmaß behandelt. Die dort formulierten Ziele der „Rückgewinnung der technologischen Souveränität“ und des Ausbaus Deutschlands zum „Verschlüsselungsstandort Nr. 1“ lassen sich nur vor dem Hintergrund der Snowden-Veröffentlichungen erklären. Auch die seit 2014 laufende Aufarbeitung der NSA-Aktivitäten durch den Untersuchungsausschuss des Deutschen Bundestages haben diese politische Schwerpunktsetzung verfestigt. Einen weiteren Schub erhielt die politische Diskussion durch das Bekanntwerden eines Cyber-Angriffs auf den Deutschen Bundestag im Sommer 2015. Über mehrere Monate war ein Angreifer im Netz des Parlaments und konnte Daten im Umfang von 16 Gigabyte aus den Büros von Abgeordneten entwenden. Deutsche Sicherheitsbehörden schreiben den Angriff russischen Nachrichtendiensten zu.

Die Verabschiedung mehrerer Gesetze zur IT- und Cybersicherheit, die Bereitstellung erheblicher Haushaltsmittel für mehr IT-Sicherheit sowie der Ausbau aller relevanten Sicherheitsbehörden durch deutlich mehr Personal waren unmittelbare Folgen von Snowden-Veröffentlichung und Bundestagsangriff.



Thyssen Hack

ThyssenKrupp hat 2016 öffentlich einen Hack des eigenen Netzwerks eingeräumt. Der Essener Konzern vermutete hinter dem Angriff eine Industriespionage-Aktion aus Südostasien. Ziel des Angriffes war vermutlich der Diebstahl von technischem Know-how zu innovativen Produktionsprozessen. Bei einem Projekt im Geschäftsbereich Industrial Solutions, der sich mit dem Bau industrieller Großanlagen beschäftigt, war dieser Diebstahl sogar erfolgreich.

Entdeckt wurde die Spionageaktion durch das firmeninterne Computer Emergency Response Team (CERT) – einer Spezialeinheit für die Cyber-Sicherheit im Großkonzern. CERT-Einheiten sind firmenübergreifend organisiert. In dem internationalen Dachverbund der CERTs, „FIRST“, sind insgesamt 366 Teams aus 78 Staaten registriert. Die meisten dieser Teams sind staatlich organisiert und im akademischen und militärischen Bereich aktiv. Unternehmen greifen häufig alternativ auch auf externe IT-Einheiten zurück.

Cybersicherheitslage in Deutschland

Die zentrale IT- und Cybersicherheitsbehörde Deutschlands, das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn, veröffentlicht einmal jährlich einen Lagebericht zur IT-Sicherheit. Im jüngsten Bericht beschreibt das BSI nicht nur eine technisch komplexer gewordene Bedrohungssituation, sondern auch eine Vielzahl von unterschiedlichen Angriffen gegen Einrichtungen in Deutschland („Die Lage der IT-Sicherheit in Deutschland 2016“). Ransomware in Krankenhäusern, Cyberspionage in Rüstungskonzernen, gezielte Spear-Phishing-Attacken gegen Regierungsbedienstete und Schadsoftware in Atomkraftwerken sind nur einige der Beispiele, die im letzten Jahr vom BSI registriert wurden. Ein gleichbleibend hohes Angriffsniveau auf Regierungseinrichtungen, gravierende Fälle von Cyberspionage in Großunternehmen und erste substanzielle Fälle von Angriffen auf kritische Infrastrukturen kennzeichnen die Gesamtlage. Ergänzt

werden die Feststellungen des BSI durch das Bundeslagebild Cybercrime, welches das Bundeskriminalamt (BKA) einmal jährlich veröffentlicht, zuletzt im Sommer 2016 für das Vorjahr („BKA Cybercrime Bundeslagebild 2015“). Zwar liegen dort die offiziell erfassten, das heißt bei der Polizei angezeigten Fälle von Cybercrime-Delikten mit 46.000 Fällen etwas unter den Zahlen des Vorjahres. Die durch die Delikte entstandenen Schäden sind jedoch leicht gestiegen. Zudem geht das BKA von einer sehr hohen Dunkelziffer aus und sieht insbesondere die spürbar zunehmenden Aktivitäten der organisierten Kriminalität auf diesem Feld mit großer Sorge.

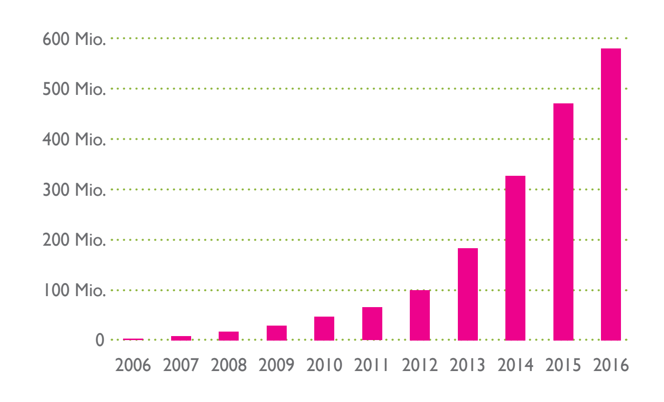
Cybersicherheitsstrategie

Eine erste Cybersicherheitsstrategie hatte die deutsche Bundesregierung bereits im Jahr 2005 beschlossen. Der vom Bundesinnenministerium erarbeitete „Nationale Plan zum Schutz der Informationsinfrastrukturen“ setzte klare Schwerpunkte bei der Prävention und dem Aufbau von Fähigkeiten auf dem Feld der IT-Sicherheit. Wichtige Maßnahmenbereiche sind der Ausbau des Sicherheitsbewusstseins, Infrastrukturinvestitionen, die Ertüchtigung des BSI sowie Wissenschaft und Forschung. Der „Nationale Plan“ war noch vollständig zivil ausgerichtet. Auch die nachfolgende Strategie der Bundesregierung, die „Cybersicherheitsstrategie für Deutschland“ aus dem Jahr 2011, war eine weitgehend präventive und zivile Strategie. Im Mittelpunkt stand der Schutz kritischer Infrastrukturen und anderer wichtiger IT-Systeme. Erstmals wurden rechtliche Verpflichtungen von Betreibern von Infrastrukturen zum Schutz der IT ihrer Systeme angekündigt. Ebenfalls zum ersten Mal wurden ressortübergreifende Strukturen für die Bearbeitung der Cybersicherheit eingerichtet: ein „Nationaler Cybersicherheitsrat“ als strategisches Steuerungsgremium und das Cyberabwehrzentrum im BSI als operative Zusammenarbeitsplattform der Sicherheitsbehörden. Militärische Cyberabwehr spielt wiederum nur eine kleine Rolle am Rande. Die Strategie von 2011 läutet eine Diskussion über deutsche und europäische Industriepolitik auf dem Feld der IT-Sicherheit ein, indem sie „technologische Souveränität und wissenschaftliche Kapazität Deutschlands“ als wichtige Voraussetzung für langfristige Gewährleistung der IT- und Cybersicherheit benennt.

Mit der Fortschreibung der Cybersicherheitsstrategie im Jahr 2016 nehmen Fragen der Cyberverteidigung einen größeren Stellenwert ein. Die Verteidigungsfähigkeiten der Bundeswehr im Cyberraum werden als wesentlicher Teil der Cybersicherheitsarchitektur angesehen. Dementsprechend werden sowohl der Ausbau militärischer Fähigkeiten als auch die engere Zusammenarbeit von zivilen und militärischen Stellen gefordert.

Mit der Fortschreibung der Cybersicherheitsstrategie im Jahr 2016 nehmen Fragen der Cyberverteidigung einen größeren Stellenwert ein.

Gesamtentwicklung von Schadprogrammen in den letzten 10 Jahren



Quelle: AV-Test Sicherheitsreport 2015-2016

Wesentlichen Stellenwert nimmt in der Strategie auch die Zusammenarbeit von Staat und Wirtschaft bei der Cybersicherheit ein. Schwerpunkte sind die Stärkung der Kooperation mit Providern, die Förderung nationaler IT-Sicherheitsunternehmen und die Errichtung gemeinsamer Plattformen für Informationsaustausch. Eine Stärkung operativer Fähigkeiten der Sicherheitsbehörden und ihr Einsatz auch zum Schutz der deutschen Wirtschaft runden die neue Strategie ab.

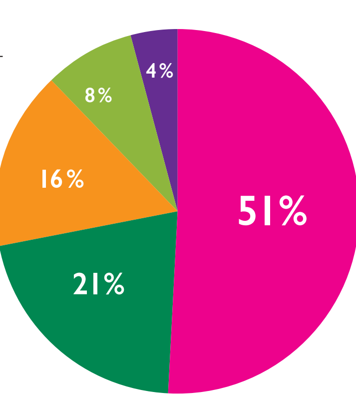
Insgesamt hat die dritte deutsche Cybersicherheitsstrategie auch im internationalen Vergleich schon einen hohen Reifegrad erreicht, wenngleich manche Zielstellungen, insbesondere industrie- und technologiepolitischer Art, 2016 zum wiederholten Mal in der Strategie aufgegriffen werden, konkrete Umsetzungsmaßnahmen aber weiterhin nur sehr allgemein beschrieben werden. Schwerpunkte der aktuellen Cybersicherheitspolitik des Bundes sind der Strategie entsprechend die Gesetzgebung und der Ausbau behördlicher und kooperativer operativer Strukturen.

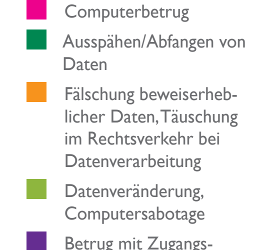
IT-Sicherheits-Gesetzgebung

IT-Sicherheit ist in Deutschland seit Gründung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auch ein gesetzgeberisches Thema. Mehrere Novellen des BSI-Gesetzes haben die Befugnisse der Behörde erweitert, etwa 2009 im Hinblick auf operative Aufgaben zum Schutz der IT der Bundesregierung. Mit der 2012 begonnenen und 2015 zum Abschluss gekommenen Debatte um ein IT-Sicherheitsgesetz hat Deutschland einen gesetzgeberisch großen Schritt nach vorn getan. Weitgehend parallel und in Wechselwirkung zu der europäischen Diskussion über eine Richtlinie zum Schutz der Netz- und Informationssicherheit (NIS directive) hat Deutschland ein IT-Sicherheitsgesetz beschlossen, das zentrale Akteure der Digitalisierung, die Infrastrukturbetreiber und die Anbieter digitaler Dienste, in die Pflicht nimmt: Mit dem im Sommer 2015 verabschiedeten und bis 2018 umzusetzenden Gesetz wird von den Unternehmen verlangt, dass sie ihre IT nach dem „Stand der Technik" absichern und Vorfälle an die Behörden melden. Gleichzeitig werden die Befugnisse des BSI zur

Sammlung von Informationen, Warnung von Betroffenen oder Untersuchung von Produkten erweitert. Deutschlands ‚Vorpreschen' mit dem IT-Sicherheitsgesetz hat die europäische Gesetzgebung sichtbar beeinflusst. Im Sommer 2016 verabschiedeten Europäisches Parlament und Rat die NIS-Richtlinie, die von der Regelungsmethode und der Reichweite her dem deutschen IT-Sicherheitsgesetz sehr nahekommt, ein wenig aber darüber hinausgeht: Betreiber kritischer Infrastrukturen müssen sich nach europäischem Recht etwas stärker kontrollieren lassen, und auch für einige besonders wichtige digitale Dienste – Suchmaschinen, Online-Marktplätze, Cloud-Dienste – gelten strengere IT-Sicherheitsvorschriften als in Deutschland. Deutschland hat insgesamt aber nur geringe Notwendigkeit, sein bestehendes Gesetz zu ändern, um europäisches Recht umzusetzen.

Cybercrime im engeren Sinne 2015 (prozentuale Verteilung)





Quelle: BKA, Bundeslagebild Cybercrime 2015

Im Schatten von IT-Sicherheitsgesetz und NIS-Richtlinie haben Aspekte der IT- und Cybersicherheit mittlerweile breit Eingang gefunden in deutsche Gesetze und Verordnungen. Im Telekommunikationsrecht, Energierecht, Gesundheitswesen, Atomgesetz und vielen anderen Rechtsvorschriften werden bereichsspezifische Vorgaben für die IT-Sicherheit der dort genutzten Systeme gemacht, nicht immer widerspruchsfrei zum IT-Sicherheitsgesetz, in den allermeisten Fällen aber unter Rückgriff auf die Expertise des BSI, als fachlich übergreifende Klammer deutscher IT-Sicherheitsvorschriften.

Organisation der Cybersicherheit, wichtige Akteure

Das BSI hat in der deutschen Cybersicherheitsorganisation eine herausragende Stellung. Die 1991 gegründete Behörde ist in nahezu alle Prozesse eingebunden und in vielen Fällen federführend. Weit über die Rolle einer technischen Fachbehörde hinaus ist das BSI in den letzten Jahren zur speziellen Abwehrbehörde für Angriffe auf die Regierung, zum Regulierer der Cybersicherheit in vielen Bereichen der Gesellschaft, zum Federführer bei der Koordinierung der Cyberabwehr im Cyberabwehrzentrum und zum technologiepolitischen Impulsgeber geworden. Das BSI wird in Gesetzgebungsverfahren ebenso einbezogen wie in technische Standardisierung, in alle nennenswerten IT-Projekte des Bundes und die Abwehr aller größeren Cyberangriffe. Von 2002 bis 2016 hat sich der Personalbestand des BSI dementsprechend verdreifacht auf heute über 800 Mitarbeiter.

Aber auch die anderen Sicherheitsbehörden des Bundes entwickeln ihre Cyberfähigkeiten weiter. Das Bundeskriminalamt hat seine Gruppe

Cybercrime deutlich ausgebaut. Das Bundesamt für Verfassungsschutz hat im Bereich der Spionageabwehr eine Unterabteilung für Cyberspionage und -sabotage gegründet. Auch der Bundesnachrichtendienst hat mit der „Strategischen Initiative Technik“ seine Fähigkeiten zur Aufklärung im Cyberraum erweitert. Mit der Anfang 2017 erfolgten Gründung der „Zentralstelle für IT im Sicherheitsbereich“ (ZITIS) in München entsteht eine neue Behörde, die für Sicherheitsbehörden des Bundes technische Mittel und Fähigkeiten bereitstellen soll, um im Cyberraum wirksamer handeln zu können. Im Einklang mit der strategischen Erweiterung der Cybersicherheit um militärische Cyberverteidigung hat die Bundeswehr Anfang 2017 ein Kommando Cyber- und Informationsraum (CIR) eingerichtet. Diese militärische Organisationseinheit mit eigenem Inspekteur und bis zu 13.000 Soldaten soll neben Heer, Marine und Luftwaffe Teil der deutschen militärischen Verteidigungsarchitektur werden. Mit einer entsprechenden Neuorganisation des Ministeriums und der Schaffung von Ausbildungs- und Forschungskapazitäten an der Bundeswehruniversität hat die militärische Cyberverteidigung einen erheblichen Sprung nach vorn getan.

Deutliches Wachstum erfahren in Deutschland in letzter Zeit Gemeinschaftseinrichtungen der Wirtschaft sowie Kooperationsprojekte von Staat und Wirtschaft.

Hinter diesen Anstrengungen des Bundes wollen auch die Bundesländer nicht zurückbleiben und haben in ihrer Mehrzahl den Aufbau spezieller Organisationseinheiten der Cybersicherheit beschlossen oder begonnen, sei es im Bereich technischer IT-Sicherheit (zum Beispiel CERTs), im Bereich der Polizeien (Zentralstellen für Cybercrime) oder des Verfassungsschutzes. Eine einheitliche Behördenarchitektur der Cybersicherheit ist in den deutschen Ländern bislang nicht zu erkennen. Der erhebliche Auf- und Ausbau von sicherheitsbehördlichen Strukturen stößt auf zwei zentrale Probleme: zum einen die an vielen Schnittstellen der Behörden noch weitgehend ungeklärte Zuständigkeitsverteilung, zum anderen die erhebliche Schwierigkeit, in den Strukturen des öffentlichen Dienstes qualifiziertes Cybersicherheitspersonal zu finden.

Deutliches Wachstum erfahren in Deutschland in letzter Zeit Gemeinschaftseinrichtungen der Wirtschaft sowie Kooperationsprojekte von Staat und Wirtschaft. Angefangen mit dem eher der Awareness dienenden Verein „Deutschland sicher im Netz“ (2006) über die Zusammenarbeitsplattform „UP KRITIS“ (2007) zum Schutz kritischer Informationsinfrastrukturen, den strategischen Cybersicherheitsrat (2011) bis zur dem Informationsaustausch dienenden Allianz für Cybersicherheit (2012) und der operativen Gesellschaft „Deutsche Cybersicherheits-Organisation“ (2015) existieren eine Fülle von Einrichtungen, in denen gemeinsam an Cybersicherheit in und für Deutschland gearbeitet wird. ■

Unterschiedliche Prioritäten

Die Durchsetzung nationaler Sicherheitsinteressen im digitalen Raum kann IT-Sicherheit und Menschenrechte beeinträchtigen. Cybersecurity ist deshalb international nicht nur ein Thema für die technische Community, sondern auch für die Zivilgesellschaft.

ISABEL SKIERKA

Die Enthüllungen von Edward Snowden im Juni 2013 haben international eine breite öffentliche Debatte zum Thema Cybersicherheit angestoßen und Forderungen Nachdruck verliehen, nationale Sicherheitsinteressen nicht auf Kosten der technischen Sicherheit des Internets und damit der Sicherheit von Nutzern durchzusetzen. Spätestens seit diesen Ereignissen ist deutlich, dass Cybersicherheit nicht von Staaten allein, sondern nur in Kooperation mit Unternehmen, Wissenschaft und Zivilgesellschaft verantwortet werden kann. Cybersicherheit steht für den Schutz des Internets, damit vernetzter IT-Systeme und der darüber transportierten und gespeicherten Informationen. Bedrohungen reichen vom Diebstahl von

Informationen oder der Veränderung von Daten bis zur Sabotage von Infrastrukturen. Bei der Bekämpfung von Cyberkriminalität geht es um den Schutz vor illegalen Handlungen, die sich Computernetzwerken oder Informationssystemen als Mittel bedienen oder sich gegen diese richten. Auch von Cyberterrorismus und Cyberkrieg ist oft die Rede. Zwar setzen Kriegsparteien schon heute Cyberangriffe gemeinsam mit konventionellen Angriffen gegeneinander ein. Einen Krieg, der ausschließlich im digitalen Raum geführt wird, gab es bisher jedoch noch nicht.

Cybersicherheit steht für den Schutz des Internets, damit vernetzter IT-Systeme und der darüber transportierten und gespeicherten Informationen.

Die Debatte um Cybersicherheit und die verschiedenen Positionen der Stakeholdergruppen spiegeln immer auch ein unterschiedliches Verständnis von Cybersicherheit und unterschiedliche Prioritäten wider. Drei Dimensionen von Sicherheit stehen dabei im Vordergrund. Sie werden von den verschiedenen Erscheinungsformen von Cybersicherheits-Beeinträchtigungen in unterschiedlichem Maß tangiert: 1) die technische Sicherheit von Netzwerken und Geräten im Sinne des Schutzes von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; 2) die nationale Sicherheit von Staaten und ihren Bevölkerungen; 3) die individuelle Sicherheit der Nutzer von Informations- und Kommunikationstechnologien (IKT), einschließlich der Wahrung ihrer Menschenrechte. Obwohl diese verschiedenen Aspekte von Cybersicherheit eng miteinander verknüpft sind, können sie oft im Konflikt zueinander stehen. Hieraus resultiert auch die hohe gesellschaftspolitische Relevanz des Themas.

Der nachfolgende Überblick bietet eine Zusammenfassung der wichtigsten internationalen Gremien, Institutionen und Prozesse zu Cybersicherheit.

Regulatorische Rahmenwerke für Cybersicherheit

Bisher besteht kein internationales rechtlich verbindliches Regelwerk für IT- oder Cybersicherheit. Am nächsten kommen dem die Budapester Konvention zu Cyberkriminalität oder die 2016 verabschiedete IT-Sicherheitsrichtlinie der EU.

IT-Sicherheitsgesetzgebung in der Europäischen Union (EU)

Die EU entwickelt sich zu einer zunehmend einflussreichen Gesetzgeberin auf dem Gebiet der Cybersicherheit. Einheitliche Regeln für die Sicherheit von IKT und kritischen Infrastrukturen innerhalb Europas sind eine wesentliche Grundlage für die Integration des europäischen digitalen Binnenmarkts. Im Jahr 2004 erschuf die EU die „European Network and Information Security Agency" (ENISA), welche seitdem den Austausch von Informationen zu Cybersicherheit und ‚Best Practices' zwischen den Mitgliedsstaaten koordiniert und eigene politische Empfehlungen zur Verbesserung der Cybersicherheit in der EU gibt. Sie hat jedoch keine juristisch verbindliche Entscheidungsgewalt. Im Jahr 2013 veröffentlichte die EU ihre erste Cybersicherheitsstrategie zu zivilen und militärischen Aspekten der Cybersicherheit. Und im Sommer 2016 verabschiedete sie schließlich ihr erstes IT-Sicherheitsgesetz für kritische Infrastrukturen und Anbieter bestimmter digitaler Dienste: die EU-Richtlinie über Netzwerk- und Informationssicherheit (NIS-Richtlinie). Bis Mai 2018 müssen alle EU-Mitgliedsstaaten diese europäische Richtlinie in das jeweilige nationale Recht umsetzen. Deutschland implementierte die NIS-Richtlinie durch das im Sommer 2015 verabschiedete IT-Sicherheitsgesetz (siehe: Cybersicherheit in Deutschland).

> Angriffe durch oder gegen das Internet der Dinge können im Ernstfall auch Auswirkungen auf Leib und Leben haben. IT-Sicherheitsrisiken im Internet der Dinge sind ein zentrales Thema in fast allen internationalen Cybersicherheitsdiskussionen.

Auch andere Gesetze der EU, wie die 2016 verabschiedete Datenschutzgrundverordnung und die ergänzende ePrivacy-Richtlinie, haben einen wesentlichen Einfluss auf die Cybersicherheit. Die EU will und wird auch in Zukunft regulatorische Standards für IT-Sicherheit setzen. Insbesondere mit der fortschreitenden Vernetzung von Milliarden von Geräten im Internet der Dinge (Internet of Things, IoT) werden die Herausforderungen für die globale IT-Sicherheit massiv wachsen (siehe den Beitrag von Jürgen Geuter in diesem Band). Viele der ‚smarten', mit dem Internet verbundenen Geräte weisen gravierende Sicherheitslücken auf und sind daher über das Internet leicht angreifbar. In jüngster Vergangenheit haben Hacker vermehrt kompromittierte Geräte genutzt, um Denial-of-Service-Angriffe auf kritische Internetdienstleister zu verüben. Angriffe durch oder gegen das Internet der Dinge können im Ernstfall auch Auswirkungen auf Leib und Leben haben. Systemische IT-Sicherheitsrisiken im Internet der Dinge sind daher ein zentrales Thema in fast allen internationalen Cybersicherheitsdiskussionen. In Zukunft ist deshalb in Europa mit stärkeren Regulierungsmaßnahmen für das Internet der Dinge zu rechnen, zum Beispiel verbindliche

IT-Sicherheitsmindestanforderungen für Hersteller der Geräte oder eine Verschärfung der Haftungsregelungen für Software.

Internationale Kooperation zu Cyberkriminalität

Häufige Genres von Cyberkriminalität sind der Computerbetrug (wie zum Beispiel Transaktionen unter Nutzung missbräuchlich erlangter Kredikarten-daten), und das Ausspähen und Abfangen von Daten (Phishing). Weitere Genres sind die Verbreitung von illegalen Inhalten, Spam und Malware, das Lancieren von Denial-of-Service-Angriffen, Online-Erpressung und andere rechtswidrige Aktivitäten (vgl. Bundeslagebild Cybercrime 2015). Die durch Cyberkriminalität verursachten Schäden belaufen sich Schätzungen zufolge auf etwa 450 Milliarden US-Dollar pro Jahr, mit steigender Tendenz (World Econ. Forum: *Global Risks Report*).

Inzwischen kooperieren Strafverfolgungs- und Ordnungsbehörden verschiedener Länder auf bilateraler Ebene oder multilateral innerhalb internationaler Institutionen wie Interpol, Europol, Ameripol und Aseanapol. Dabei ist die Zusammenarbeit mit Internetkonzernen und privaten Unternehmen unabdinglich.

Die wichtigste internationale rechtliche Grundlage zur Bekämpfung von Cyberkriminalität ist die „Budapest Convention on Cybercrime" des Europarats. Sie wurde 2001 verabschiedet und trat 2004 in Kraft. Bisher haben 56 Staaten weltweit (zum größten Teil europäische Länder, aber auch Länder wie Australien, Japan und die USA) die Konvention unterschrieben, 52 haben sie ratifiziert. Ziel ist die Harmonisierung des Strafrechts und der Strafverfahren sowie die Verbesserung internationaler Zusammenarbeit im Bereich der Internetkriminalität.

Auch wenn die Budapester Konvention sowie bilaterale Abkommen zu einer Verbesserung der Kooperation zwischen den Mitgliedsstaaten beitragen, definiert dennoch jedes nationale Rechtssystem Cyberkriminalität und rechtswidrige Aktivitäten unterschiedlich. Überdies haben wichtige Länder wie Russland, China, Indien und Brasilien die Konvention nicht unterschrieben.

Im Jahr 2014 hat auch die Afrikanische Union (AU) eine Konvention zu Cybersicherheit und Datenschutz verabschiedet. Sie schafft ein allgemeines rechtliches Regelwerk für E-Commerce, Datenschutz, Cybersicherheit und Cyberkriminalität. Bisher hat jedoch kein AU-Mitgliedsstaat die Konvention ratifiziert. Außerdem ist das Regelwerk umstritten, da einige seiner

Inhalte zur Einschränkung von Menschenrechten, Diskriminierung und zu mehr staatlicher Kontrolle über das Internet missbraucht werden könnten.

Die politisch-militärische Dimension: Cyberterrorismus und Cyberkrieg

Immer mehr Staaten entwickeln politisch wie militärisch offensive und defensive Cyberfähigkeiten, die zunehmend in internationalen Konflikten zum Einsatz kommen. In einigen Regionen hat dies bereits zu einem derartigen digitalen Wettrüsten geführt, dass die internationale Sicherheit im digitalen Raum zunehmend gefährdet ist. Daher wäre es sehr wichtig, dass sich die Regierungen auf gemeinsame internationale Normen, Regeln und Prinzipien für ein verantwortungsvolles Staatenverhalten im digitalen Raum einigen.

Es ist wichtig, dass sich die Regierungen auf gemeinsame internationale Normen, Regeln und Prinzipien für ein verantwortungsvolles Staatenverhalten im digitalen Raum einigen.

Auf internationaler Ebene sind die Vereinten Nationen (VN) das Hauptforum, in dem Regierungen Normen und Regeln für die internationale Sicherheit im digitalen Raum verhandeln. Neben den internationalen Verhandlungen in den VN sind auch regionale multilaterale Organisationen wie die Organisation für Sicherheit und Zusammenarbeit (OSZE), die Organisation des Nordatlantikvertrags (NATO) oder der Verband südasiatischer Nationen (ASEAN) wichtige Foren zur Verhandlung von Cybersicherheit.

Akteure

Die Vereinten Nationen

In den VN begannen die Verhandlungen um Cybersicherheit bereits 1998, als Russland einen Resolutionsentwurf in den ersten VN-Ausschuss für Abrüstung und internationale Sicherheit einbrachte, der die von Informations- und Kommunikationstechnologien (IKT) ausgehende Bedrohung für die internationale Sicherheit anerkannte. Zu einer Einigung auf eine abschließende Resolution kam es jedoch in der VN-Generalversammlung damals nicht. 2004 wurde zum ersten Mal eine Gruppe von Regierungssachverständigen für „Entwicklungen auf dem Gebiet der Informationstechnik und der Telekommunikation im Kontext der internationalen Sicherheit" einberufen, auch „Group of Governmental Experts" genannt (GGE). Die bisher vier UN-GGEs untersuchen bestehende sowie potenzielle Bedrohungen für die internationale Sicherheit und den Frieden, die aus

der Nutzung von IKT erwachsen. Ein Meilenstein war der 2013 erreichte GGE-Konsens, dass das Völkerrecht sowohl online als auch offline Anwendung finden muss. Zu einem ähnlichen Zeitpunkt, 2012, beschloss auch der UN-Menschenrechtsrat, dass Menschenrechte offline sowie online zu schützen sind. Der letzte Bericht der vierten Gruppe im Jahr 2015 enthält eine Reihe von spezifischeren Normen, zum Beispiel zum Schutz von kritischen Infrastrukturen sowie von autorisierten digitalen Notfallteams. Eine neue, fünfte GEE mit 25 Mitgliedsstaaten tagt seit Herbst 2016. Es bleibt abzuwarten, ob die GGE- und VN-Mitgliedsstaaten die Erkenntnisse und Bestimmungen aus den früheren Berichten konkretisieren und umsetzen werden, um das Sicherheitsumfeld im digitalen Raum tatsächlich zu verbessern. Eine spannende Frage bleibt, wie sich die UN-GGE institutionell weiterentwickeln wird und ob sie zukünftig auch nicht staatliche Stakeholder aus der Industrie, der Zivilgesellschaft und aus dem technischen Umfeld mit einbeziehen kann und wird.

Die Verhandlungen in den VN und anderen Institutionen sind schon immer von Unstimmigkeiten zwischen westlichen Staaten auf der einen Seite und meist von China und Russland angeführten Koalitionen auf der anderen Seite geprägt. Die Shanghaier Organisation für Zusammenarbeit (SCO), zu der unter anderem China und Russland zählen, erarbeitete 2011 innerhalb der VN einen Resolutionsentwurf für einen „Internationalen Verhaltenskodex für die Informationssicherheit", der unter anderem dafür kritisiert wurde, Kontrollmöglichkeiten von Regierungen über das Internet stärken zu wollen. Viele westliche Staaten lehnten den Entwurf ab. Ähnliche Konflikte treten auch innerhalb der Internationalen Fernmeldeorganisation (ITU) auf, einer zwischenstaatlichen VN-Organisation, die sich weltweit mit technischen Aspekten und Standards der Telekommunikation beschäftigt. Einige Mitgliedsstaaten, unter anderem China, Russland, Saudi-Arabien und die Vereinigten Arabischen Emirate (VAE), versuchen gleichermaßen regelmäßig wie hartnäckig die Zuständigkeiten der ITU, und damit der Regierungen, auf Cybersicherheit und Digitalpolitik zu erweitern. Bisher bleibt die Rolle der ITU in diesen Bereichen jedoch auf die eines Diskussionsforums beschränkt.

Die Verhandlungen in den Vereinten Nationen und anderen Institutionen sind schon immer von Unstimmigkeiten zwischen westlichen Staaten auf der einen Seite und meist von China und Russland angeführten Koalitionen auf der anderen Seite geprägt.

Die Verabschiedung eines internationalen, rechtlich verbindlichen Cybersicherheitsvertrags ist mindestens auf mittelfristige Sicht unwahrscheinlich. Zu groß sind die Unterschiede der Interessen verschiedener Staaten in der

internationalen Gemeinschaft. Mit den aktuellen geopolitischen Konflikten in der Ukraine und Syrien, dem Abkühlen der Beziehungen zwischen den USA und Russland und den neuen Anschuldigungen westlicher Staaten gegen Russland, seine Cyberfähigkeiten offensiv für Angriffe und Desinformationskampagnen zur Störung der Fundamente westlicher Demokratien einzusetzen, scheint eine Einigung auf einen Cybersicherheitsvertrag bis auf Weiteres ausgeschlossen.

Regionale Foren

Auch andere regionale Organisationen nehmen sich der politisch-militärischen Dimension von Cybersicherheit an. Die Mitgliedsstaaten der NATO haben im September 2014 eine Cyber Defense Policy verabschiedet, die Cyber-Bedrohungen als potenzielle Quelle einer kollektiven Verteidigung gemäß Artikel 5 des NATO-Vertrags nennt und Richtlinien für die Umsetzung einer gemeinsamen Cyber-Verteidigungspolitik im Bündnis setzt. Rechtsexperten eines von der NATO gegründeten Center of Excellence erarbeiteten außerdem 2013 in Kooperation mit dem Internationalen Roten Kreuz und dem Cyber-Kommando der US-Armee ein Handbuch über Cyberkrieg, das *Tallinn Manual*. Das Handbuch enthält 95 Regeln, an denen sich NATO-Staaten im Fall eines Cyberkriegs orientieren können. Es ist jedoch kein offizielles NATO-Dokument. Das im Februar 2017 veröffentlichte neue *Tallinn Manual 2.0* setzt sich auch mit konkreten Fragen zu Angriffen auseinander, die unter der Schwelle von bewaffneten Angriffen bleiben. Zudem arbeitet in der OSZE seit 2012 eine informelle Arbeitsgruppe an der Konkretisierung von vertrauenswürdigen Maßnahmen im Cybersicherheitsbereich. Ebenfalls will ASEAN sich 2017 stärker über regionale Normen für Cybersicherheit austauschen und seine Kooperation im Bereich Cyber-Kapazitätsaufbau und Cybersicherheit ausbauen.

Multistakeholder-Governance-Prozesse und Cybersicherheit

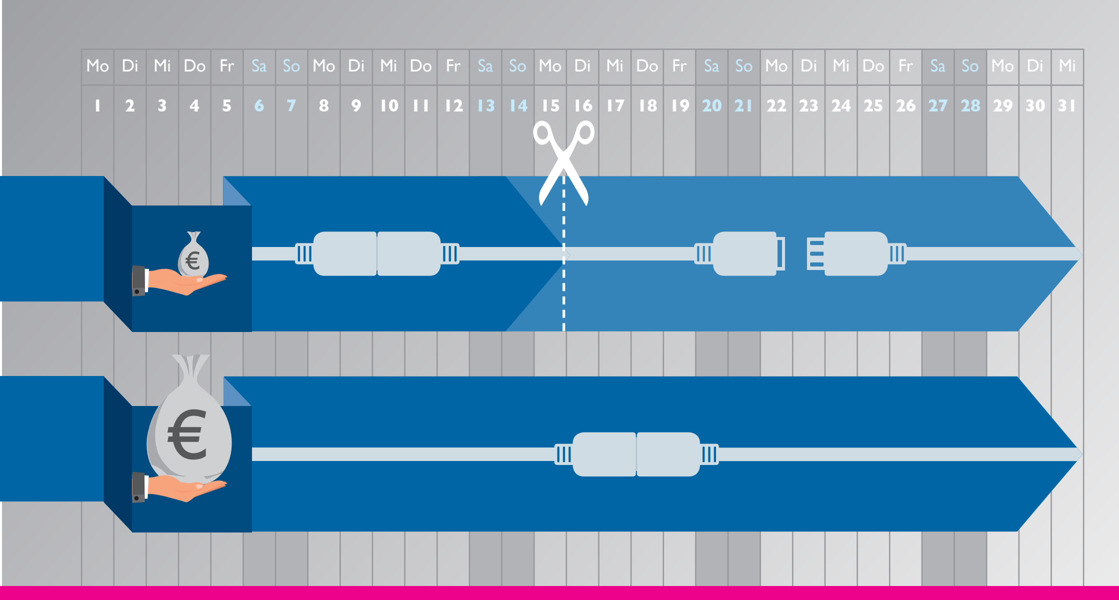
Die meisten ‚Governance'-Prozesse zu Cybersicherheit finden also zwischen Staaten und selten unter Einbeziehung anderer Stakeholder statt. Dieser Eindruck täuscht jedoch darüber hinweg, dass insbesondere der technische und damit grundlegendste Aspekt von Cybersicherheit seit der Entstehung des Internets in den Händen von Ingenieuren, Informatikern und anderen Technikern liegt. Diese haben sich schon immer international in losen Netzwerken ausgetauscht. Digitale Notfallteams für Organisationen oder ganze Länder, sogenannte Computer Security Incident Response Teams CSIRTs, auch als CERTs bekannt), kooperieren schon

seit Ende der 1980er-Jahre miteinander, um das Internet gegen Cyberangriffe zu verteidigen. Über 200 CSIRTs und IT-Sicherheitsunternehmen haben sich im internationalen „Forum for Incident Response and Security Teams" (FIRST) zusammengeschlossen. Auch in internationalen Standardisierungsgremien, in der Internet Engineering Task Force (IETF), in dem Institute of Electrical and Electronics Engineers (IEEE), dem World Wide Web Consortium (W3C) und natürlich in großen Technologiekonzernen wie Google setzen technische Experten Standards, um das Internet sicherer zu machen.

Zahlreiche zivilgesellschaftliche und Menschenrechtsorganisationen beschäftigen sich auf nationaler und internationaler Ebene mit Cybersicherheit und bringen ihre Positionen immer erfolgreicher in die öffentliche Debatte ein.

Spätestens seit den Snowden-Enthüllungen ist der Druck auf Regierungen, ihre Verhandlungen transparenter zu führen und die Diskussionen auch für Zivilgesellschaft und Industrie zu öffnen, gestiegen. Erfolgt nämlich die Durchsetzung nationaler Sicherheitsinteressen im digitalen Raum auf Kosten der technischen Sicherheit von Infrastrukturen und Geräten, nehmen die Sicherheit einzelner Nutzer, ihre Menschenrechte und das Internet im Allgemeinen Schaden. Zahlreiche zivilgesellschaftliche und Menschenrechtsorganisationen beschäftigen sich deshalb auf nationaler und internationaler Ebene mit Cybersicherheit und bringen ihre Positionen immer erfolgreicher in die öffentliche Debatte ein. Das IGF hat 2016 ein „Best Practice Forum on Cybersecurity gegründet, um auch die „hard security"'-Themen von Cybersicherheit systematisch unter Mitwirkung aller wichtigen Stakeholder zu diskutieren. Einbezogen werden dabei vor allem die Sektoren Regierung, Privatwirtschaft, Zivilgesellschaft sowie Wissenschaft und technische Community. Hinzu kommen – je nach Anlass – weitere internationale Organisationen mit themenspezifischer Expertise oder Verantwortung. Ein weiterer wichtiger Prozess ist die Global Conference on CyberSpace, die die britische Regierung 2011 ins Leben rief. Sie findet regelmäßig alle ein bis zwei Jahre in verschiedenen Ländern im Multi-Stakeholder-Format statt.

Mit der fortschreitenden Digitalisierung unserer Gesellschaften wird es immer schwieriger werden, zwischenstaatliche Verhandlungen zu Cybersicherheitsthemen von öffentlichen Diskussionen und den von Multi-Stakeholdern zu trennen. Beide sind auch auf internationaler Ebene längst fest miteinander verwoben. In den nächsten Jahren wird es daher darum gehen, ob und wie sich das Multi-Stakeholder-Modell auch in Diskussionen über Cybersicherheit gegen einseitige politische Interessen durchsetzen kann. ■



Garant für Meinungsvielfalt?

Eigentlich ist der Kampf um Netzneutralität mit der neuen EU-Verordnung erledigt. Nicht erledigt hingegen sind die medienpolitischen Ziele, die in der Debatte um Netzneutralität eine Rolle spielten.

RALF GRÖTKER und FRIEDHELM GREIS

Netzneutralität steht für die gleichberechtigte (neutrale) Übertragung von Daten im Internet. Relevant ist Netzneutralität vor allem als Voraussetzung für Informationsfreiheit und die Gewährleistung von Infrastrukturen öffentlicher Meinungsbildung. Darüber hinaus wird Netzneutralität als Erfordernis für Innovation betrachtet – sowohl was innovative Geschäftsmodelle betrifft (van Schewick: „Innovationsmotor Internet“, 2006; Krämer et al.: „Net neutrality“, 2013) wie auch soziale Innovationen (Zittrain: *The Future of the Internet*, 2008): Wenn Informationsangebote von Start-ups oder kleinen und mittelständischen Unternehmen für Nutzer nicht in der gleichen Übertragungsqualität zugänglich sind wie

andere Internet-Angebote oder wenn kleinere Unternehmen für die Durchleitung ihrer Daten große Summen investieren müssen, würde dies die Marktchancen der betreffenden Unternehmen erheblich schmälern. Debatten über Netzneutralität werden über die technischen, wirtschaftlichen und juristischen Details geführt.

Formen der Nicht-Gleichbehandlung von Daten reichen von der Drosselung des Datenverkehrs bis zur Blockierung von Inhalten.

Das Prinzip der Neutralität kann unterschiedlich interpretiert werden. Strikte Neutralität würde bedeuten, dass alle Daten in jeder Hinsicht gleich behandelt werden. Bereits übliche Verfahren des Netzwerkmanagements, die von Internet Service Providern zur Vermeidung von Kapazitätsengpässen eingesetzt werden, können als Verletzung von strikter Netzneutralität betrachtet werden. Eine weniger strenge Auslegung des Neutralitätsbegriffes würde nur zur Folge haben, dass gleiche Kategorien von Daten oder Diensten (wie zum Beispiel Webseiten oder Telefonate) gleich behandelt werden. Formen der Nicht-Gleichbehandlung von Daten reichen von der Drosselung des Datenverkehrs bis zur Blockierung von Inhalten. Internet Service Provider befürworten oftmals eine Aufweichung strenger gesetzlicher Vorgaben für Netzneutralität aus wirtschaftlichen Interessen. Ein Abweichen von dem Prinzip der Netzneutralität würde es Internet Service Providern ermöglichen, Inhalte-Vermittlern wie Google, Facebook, Whatsapp oder Netflix die Weiterleitung von Daten in Rechnung zu stellen oder spezielle Premium-Dienste anzubieten. Ein gängiges Argument in diesem Kontext ist, dass die Beteiligung von Inhalte-Vermittlern (Intermediären) an den Kosten der Datenübermittlung notwendig sei, um den Ausbau der Internet-Breitbandversorgung zu finanzieren. Ein anderes Argument der Netzneutralität-Gegner besagt, dass insbesondere Dienstleistungen im Bereich des vernetzten und automatisierten Straßenverkehrs oder der Telemedizin auf die störungsfreie und schnelle Weiterleitung von Daten im Internet angewiesen seien. Daher sollte es ermöglicht werden, die entsprechenden Daten priorisiert zu behandeln – was einer Abkehr von dem Prinzip der Netzneutralität gleichkäme.

Netzneutralität

Netzneutralität war in den Jahren 2012 bis 2016 Gegenstand zahlreicher politischer Kampagnen von NGOs. Wie bei kaum einem anderen digitalpolitischen Thema ist es dabei gelungen, einem auf den ersten Blick abstrakten Gegenstand mit gestalterischen Mitteln ein pointiert zu veranschaulichen. Die Dokumentation auf dieser und den folgenden Seiten zeigt auf den folgenden Seiten einige der prägnantesten Beispiele.

Fokus: Netzneutralität und Medienpolitik

Befürworter der Netzneutralität befürchten, dass ein Abweichen der bisherigen Praxis einer weitgehenden Gleichbehandlung von Daten im Internet zu einer Einschränkung der öffentlichen und privaten Meinungsbildung führen könnte, weil Informationen nicht mehr uneingeschränkt mitteilbar wären. Betroffen, so wird argumentiert, seien davon zum einen kommunikationsrelevante Grundrechte (Peucker-Minecka: *Netzneutralität*, 2014), zum anderen die (traditionell unter die Medienpolitik subsumierte) Infrastrukturgewährleistung von Plattformen für öffentliche Kommunikation

(Grötker: *Das Bürger-Internet,* 2015). Eine konkrete Sorge: Ein Abweichen von dem Prinzip der Netzneutralität könnte dazu führen, dass Informationsinhalte, die für die öffentliche Meinungsbildung in einer demokratischen Gesellschaft relevant sind, zunehmend zentralisiert würden, das heißt, ausschließlich aus der Hand einiger großer Medienunternehmen und Inhalte-Vermittler bezogen werden könnten. Dies würde eine Verletzung von etablierten und bislang durch Instrumente der Medienpolitik gewährleisteten Standards staatlicher Meinungsmachtkontrolle gleichkommen. Strittig ist hier allerdings, welche Informationsinhalte als bedeutsam für die öffentliche Meinungsbildung erachtet werden sollten. Selbst Informationsangebote, die auf den ersten Blick eher Unterhaltungscharakter haben, können durchaus relevant sein. Dies zeigt das Beispiel der zahlreichen Proteste und Demonstrationen gegen das Anti-Produktpiraterie-Handelsabkommen ACTA, die hauptsächlich durch Musikvideos auf YouTube angestoßen worden waren. Ein anderes Beispiel für die Relevanz von vermeintlich reinen Unterhaltungsangeboten sind politisch gefärbte Arthouse-Filme, die in China über Peer-to-Peer-Netzwerke verbreitet werden, um auf diese Weise die staatliche Zensur zu umgehen.

Was die Infrastrukturgewährleistung von Plattformen für öffentliche Kommunikation betrifft, ist ein Begriff der Netzneutralität, der allein auf die physikalische Struktur der Datenübermittlung fokussiert, freilich entschieden zu eng. „Nicht-Neutralität" bei der Datenübermittlung wird gerade dann

Die „Echtes Netz"-Kampagne versuchte, die Argumentation, fehlende Netzneutralität behindere Innovation, in einem einzigen Kampagnenmotiv zu vermitteln.

https://d-64.org/wp-content/uploads/2013/05/Telekom_Kampagne_Innovation_final.png



besonders brisant, wenn sie in Kombination mit „Nicht-Neutralität“ im Umgang mit Inhalten auftritt. Die Netztheoretikerin Rebecca MacKinnon beschreibt diesen Punkt in ihrem Buch *Consent of the Networked* anhand der Praxis des Zero Rating (siehe den Beitrag von Hauke Gierow in diesem Band): Oftmals schließen Internetdiensteanbieter (vor allem Telekommunikationsdienstleister) Verträge mit Inhaltevermittlern (wie Facebook), die es den Konsumenten ermöglichen, zum Beispiel Facebook-Inhalte zu nutzen, ohne dass dies auf ihr festgesetztes Kontingent für mobile Daten angerechnet wird. Die Folge: Für Nutzer ist der Anreiz, via Facebook Informationen zu empfangen, größer als über andere Medien. Damit einher geht jedoch, dass die Nutzer den Umgang mit Inhalten sowie andere Praktiken, die Facebook seinen Nutzern vorgibt, akzeptieren müssen (siehe auch den Beitrag von Matthias C. Kettemann in diesem Band). Tatsächlich sind die Geschäftsbedingungen von Facebook alles andere als ‘neutral‘. In vielen Ländern, in denen die Regierung Bürger politisch unterdrückt, sind sie ein Problem. Facebook verlangt beispielsweise, dass Nutzer sich mit ihrem echten Namen anmelden – was Menschenrechtsaktivisten in einigen Ländern besser nicht riskieren sollten, wie das Beispiel des arabischen Bloggers Raif Badawi zeigt: Er wurde 2012 verhaftet, zu zehn Jahren Gefängnis und 1.000 Peitschenschlägen verurteilt, nachdem er eine Webseite für gesellschaftliche und politische Debatten ins Leben gerufen hatte. Ein Pseudonym wäre in diesem Fall kein Ausweg, denn dann könnte die Facebook-Präsenz wegen Verletzung der Geschäftsbedingungen jederzeit vom Netz genommen werden.



Wahrscheinlich eines der plastischsten Motive der Befürworter der Netzneutralität.

https://cdn.netzpolitik.org/wp-upload/Digiges_nn_postkarte_auto.png

Prozesse

Netzneutralität im engeren Sinne – bezogen auf die physische Struktur der Datenübermittlung – war vor allem in den Jahren 2013 bis 2016 Gegenstand politischer Prozesse auf Bundes- wie europäischer Ebene.

In Deutschland machte 2013 die „Drosselkom“-Affäre Schlagzeilen, als Pläne der Deutschen Telekom bekannt wurden, Neukunden nur noch eine Internet-Flatrate mit begrenztem Datenvolumen anzubieten. Inner-

halb weniger Tage erhielt die Bundestagspetition eines Schülers, die sich für ein Verbot der Pläne der Telekom aussprach, mehr als 50.000 Unterstützer. Der Petitionsausschuss des Bundestages befasste sich in der Folge mit dem Thema. Auch das seinerzeit von der FDP geführte Bundeswirtschaftsministerium griff die Debatte auf und legte im Sommer 2013 einen Entwurf für eine Verordnung zur Netzneutralität vor. Nach der Bundestagswahl 2013 einigten sich Union und SPD im Koalitionsvertrag, das Thema Netzneutralität im Telekommunikationsgesetz verbindlich zu regeln. Dieses Ziel wurde jedoch bereits 2014 wieder aufgegeben, weil die Entscheidung sich auf die europäische Ebene verlagert hatte.

In einer satirischen Werbeanzeige erweckte der Digitale Gesellschaft e.V. den Eindruck, das Vorgehen der Telekom ähnele Mafia-Methoden wie der Schutzgelderpressung.
https://cdn.netzpolitik.org/wp-upload/drosselkom_startups_netzneutralit%C3%A4t.jpg



Im September 2013 legte die EU-Kommission einen Vorschlag für eine neue Verordnung zum Telekommunikationsbinnenmarkt vor, die auch Regelungen zur Netzneutralität enthielt. Der Vorschlag wurde mit Änderungen unter anderem zum Schutz von Netzneutralität im April 2014 vom EU-Parlament gebilligt. Der neue Verordnungsentwurf garantierte einen weitgehenden Schutz von Netzneutralität, mit Ausnahme jedoch sogenannter Spezialdienste. Ein solcher Spezialdienst, so der Entwurf von 2014, sollte vom Prinzip der Netzneutralität dann abweichen dürfen, wenn er „über logisch getrennte Kapazitäten […] erbracht wird", wenn er „Funktionen anbietet, die durchgehend verbesserte Qualitätsmerkmale erfordern" und wenn er „als Substitut für Internetzugangsdienste weder vermarktet wird noch genutzt werden kann". Der Entwurf führte nach dem durch das Verfahren vorgegebenen Trilog zwischen Ministerrat, Parlament und Kommission zu einer Verordnung des Europäischen Parlaments, die am 27. Oktober 2015 verabschiedet wurde. Die Regelungen zu den „Spezialdiensten" wurden von der nunmehr verabschiedeten Verordnung weitgehend übernommen. Gleichzeitig wurde die Dachorganisation der europäischen Regulierungsbehörden BEREC (Body of European Regulators for Electronic Communications) damit beauftragt, bis zum August 2016 Richtlinien für die Anwendung der Verordnung zu erstellen – eingeschlossen eine genauere Definition der „Spezialdienste". Die Arbeit der BEREC wurde von einem öffentlichen Konsultationsprozess begleitet. Die Umsetzungsrichtlinie, die die BEREC 2016 veröffentlichte, folgt größtenteils der Linie der Netzneutralitäts-Befürworter. Als „Spezialdienste"

Allein mit dem Instrument der Netzneutralität werden sich die beschriebenen Probleme der drohenden Konzentration von Meinungsmacht nicht lösen lassen.

gelten nunmehr lediglich unter anderem high-quality Internet-Telefondienste (VoLTE), Telechirurgie und IPTV-Fernsehübertragungen. Die genannten Dienste dürfen nur über Netzwerke betrieben werden, die nicht an das Internet angeschlossen sind.

Nein zum 2-Klassen-Netz!
Netzneutralität ins Gesetz!

Die Kampagne "Echtes Netz – gemeinsam für Netzneutralität" beschwor ein "2-Klassen-Netz" herauf für den Fall, dass Netzneutralität nicht gesetzlich festgeschrieben würde.

https://digitalegesellschaft.de/wp-content/uploads/2013/05/plakat_03.png

Was die physikalische Struktur der Datenübermittlung betrifft, gehört das Thema Netzneutralität mit der EU-Verordnung und der Richtlinie des BEREC der Vergangenheit an. In Bezug auf Zero Rating für mobile Internetdienste stellt die Verordnung klar: Ein Internetdienstanbieter darf zwar eine Kooperation mit einem marktführenden Unternehmen wie Facebook eingehen und dabei seinen Nutzern einen Gratis-Zugang zu Facebook einräumen, während er für den Zugang zu anderen mobilen Diensten Datengebühren erhebt. Sobald der Nutzer aber sein vertraglich vereinbartes Datenvolumen aufgebraucht hat, gelten für den Zugang zu den Gratis-Diensten die gleichen Konditionen wie für alle anderen Internetverbindungen. Internetdienstanbieter haben so einen Anreiz, Datenvolumen nicht zu niedrig anzusetzen, da sie ansonsten die Kooperation mit Zero-Rating Partnern gefährden würden.



Die Kampagnen-Plattform Campact beschwor die Gefahr herauf, dass Konzerne ein Monopol auf Internetnutzung und eine Art Schnellstraße im Netz bekämen, sollte Netzneutralität nicht gesetzlich festgeschrieben werden.

https://www.campact.de/media/i/a51b39cd353d-f7d9d74d34c84981eb6c.jpg

Nicht erledigt ist mit der neuen Regelung der weitere Kreis an Problemen in Bezug auf die medienpolitischen Ziele, die in der Debatte um Netzneutralität eine Rolle spielten. Zwar nimmt die neue Regelung ausdrücklich Bezug auf die Sicherung der Meinungsvielfalt und das Recht auf freie Meinungsäußerung. Allein mit dem Instrument der Netzneutralität werden sich die beschriebenen Probleme der drohenden Konzentration von Meinungsmacht aber nicht lösen lassen. Prognosen für das Internet nach dem Jahr 2020 gehen fast unisono davon aus, dass bereits in naher Zukunft ‚das Internet' nur noch eines von vielen Netzwerken darstellen wird. Dieser Trend wird als Zersplitterung (Splintering) beschrieben. Der größere Teil dieser zukünftigen Netzwerke wird sich in den Händen privater Eigentümer befinden. Das unabhängig vom Internet betriebene Google Fiber etwa verspricht eine Verbindungsgeschwindigkeit, die bis zu hundertmal schneller ist als heutige Breitbandanschlüsse im Durchschnitt. In einigen Gegenden der USA wird der Dienst bereits angeboten. In einem solchen Szenario eines „zersplitterten Internets" wird eine gesetzliche Regulierung im Sinne der Netzneutralität, wie wir sie heute kennen und nur auf das herkömmliche Internet beziehen, von beträchtlich verminderter Wirkungskraft sein.

Eine weitere Dimension möglicher Zersplitterung betrifft die Geräte, mit denen Nutzer sich mit dem Netzwerk verbinden. Heute ist der PC immer noch die am weitesten verbreitete Allzweckmaschine. In dem Maße, wie die Internetfähigkeit von Geräten steigt, ohne dass diese dafür an einen Compu-

ter angeschlossen werden müssen, gehen Konsumenten jedoch dazu über, anstelle der Universalmaschine PC spezialisierte Geräte mit eigener Software und eigenen Anwendungen, die auf die jeweilige Aufgabe zugeschnitten sind, zu benutzen. Der weitverbreitete Gebrauch von Tablets , iPads und anderen E-Geräten zum Lesen von Onlineinhalten ist ein erster Schritt in diese Richtung. Die meisten dieser Geräte sind alles andere als ‚neutral', wie das Beispiel von Amazons E-Buch-Lesegerät Kindle zeigt: Der Kindle kann ausschließlich Dokumente im Amazon-Format wiedergeben – und diese Dokumente wiederum sind ausschließlich im Amazon-Onlinehandel erhältlich. Der Internettheoretiker Jonathan Zittrain hat für diesen Trend den Begriff der „Appliancization" (Deutsch: „Anwendungswahn") geprägt (Zittrain: *The Future of the Internet*, 2008). Der nicht neutrale Umgang mit Informationsangeboten, wie ihn Inhalte- und App-Anbieter praktizieren, tangiert nicht die Netzneutralität im Sinne der EU-Verordnung. Gleichwohl sind Meinungsvielfalt und die Gewährleistung einer Infrastruktur für öffentliche Kommunikation ebenso bedroht durch Zersplitterung und Appliancization wie durch Nicht-Neutralität in der Datenübermittlung. Politisch sind diese Themen im Bereich Plattformregulierung zu verorten. Medienpolitische Strategien, wie sie auf Bundesebene verfolgt werden, können allerdings nur sehr bedingt (wie eigentlich notwendig) auf EU-Ebene übertragen werden, da diese allein der Durchsetzung wirtschaftspolitischer Belange verpflichtet ist.



Ein so genanntes "zero rating"-Angebot des Anbieters Econet für Simbabwe, bei dem Mobilfunkkunden ihre Facebook-Nutzung nicht auf ihr Datenvolumen angerechnet wird.

https://pbs.twimg.com/media/BaD7UKfCIAAcDbD.jpg

Erwähnt werden sollte auf der anderen Seite aber ebenfalls, dass einige der politischen Ziele, für die sich Befürworter von Netzneutralität einsetzen, auch mit anderen Mitteln als staatlicher Regulierung von Verfahren der Datenübermittlung realisierbar sind. Eine Möglichkeit, Netzneutralität auf technischem Weg zu lösen, ist zum Beispiel die Einrichtung von kommunalen Netzwerken oder einer Gemeinschaftsbreitbandversorgung (Crawford: *The Wire Next Time*, 2014; Zaleski: *Is municipal broadband more important than net neutrality?*, 2014).

Akteure

Für das Prinzip der Netzneutralität machten sich in Deutschland unter anderem stark: die Digitale Gesellschaft, der Chaos Computer Club (CCC), Plattformen wie Campact.de, der Bundesverband der Verbraucher-

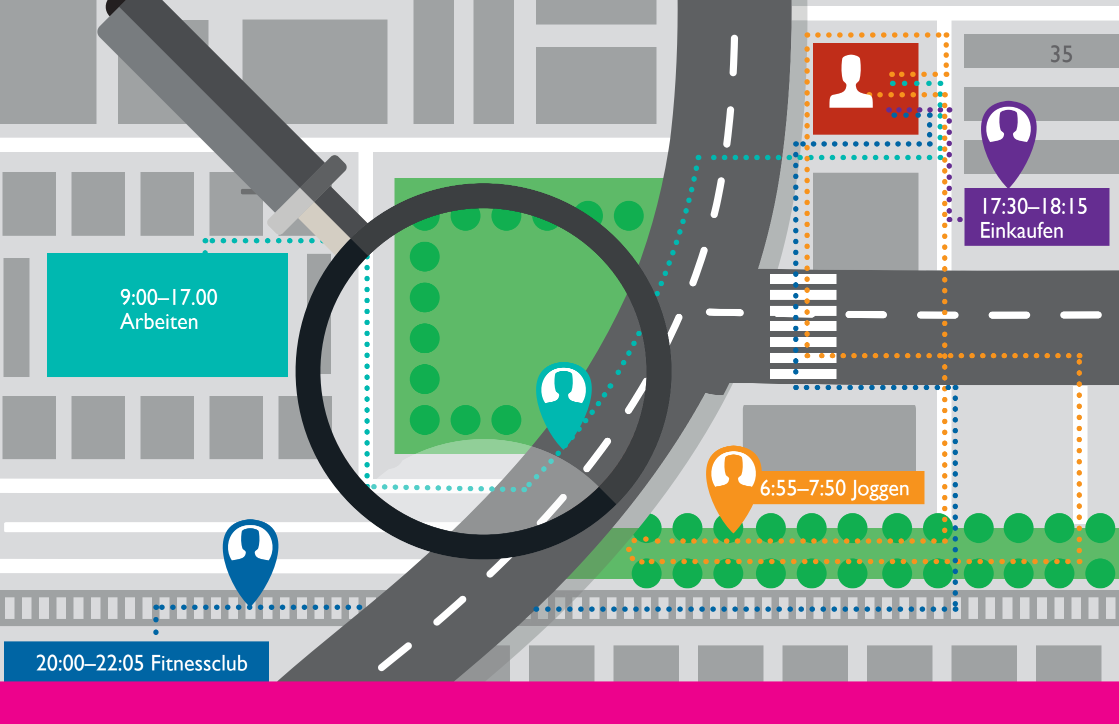
zentralen, die Journalistengewerkschaft DJV sowie die Branchenverbände Bundesverband Deutscher Zeitschriftenverleger (BDZV), der Verband Deutscher Zeitschriftenverleger (VDZ) und der Bundesverband Digitale Wirtschaft (BVDW). Gegen Netzneutralität sprachen sich vor allem die Telekommunikations- und Internet Service Provider aus, zusammengeschlossen in den Branchenverbänden Bitkom, VATM, Eco und Breko. Zu Anfang der Debatte bezog auch Bundeskanzlerin Angela Merkel öffentlich gegen Netzneutralität Stellung und forderte eine Privilegierung bestimmter Dienste, wie fahrerloser Autos oder der Telemedizin. Vonseiten der Wissenschaft wurde die Debatte begleitet von dem Rechtswissenschaftler Thomas Fetzer (Universität Mannheim) und der Rechtswissenschaftlerin Heike Schweitzer (FU Berlin). Einen ausführlichen Überblick über die Akteure bietet die Teilnehmerliste des Fachdialogs Netzneutralität, den das Bundeswirtschaftsministerium initiiert hatte (Teilnehmerliste 5. Fachdialog Netzneutralität, 2014).

Zu Anfang der Debatte bezog auch Bundeskanzlerin Angela Merkel öffentlich gegen Netzneutralität Stellung und forderte eine Privilegierung bestimmter Dienste.

Auf europäischer Ebene hatten sich zahlreiche Akteure zu der Kampagne „Save the Internet.eu“ zusammengeschlossen. Zu den Gründungsmitgliedern der Kampagne zählen EDRi, die Initiative für Netzfreiheit, die Digitale Gesellschaft, Access Now, La Quadrature du Net, Bits of Freedom and Go Veto. Zuletzt zählte die Kampagne knapp zwei Dutzend Mitgliedsorganisationen. Unterstützung erhielt die Kampagne durch Lawrence Lessig (Harvard) und Barbara van Schewick (Stanford) sowie den als Begründer des World Wide Web geltenden Informatiker Tim Berners-Lee. Von Seiten der Wirtschaft wurde die Forderung nach Netzneutralität unter anderem unterstützt durch Yahoo, eBay, Amazon und Microsoft. Gegen Netzneutralität machten sich insbesondere die Telefondienstleister stark.

Konklusion

Netzneutralität ist vor allem für den Schutz kommunikationsrelevanter Grundrechte und die Gewährleistung von Infrastrukturen öffentlicher Meinungsbildung von Belang. Darüber hinaus wird Netzneutralität unter wettbewerbsrechtlichen Aspekten als Erfordernis für Innovation betrachtet. Was die physikalische Struktur der Datenübermittlung betrifft, kann die politische Debatte um die Netzneutralität mit der EU-Verordnung und den Richtlinien der BEREC aus dem Jahr 2016 als erledigt gelten. Nicht erledigt ist mit der neuen Regelung der weitere Kreis an Problemen in Bezug auf die medienpolitischen Ziele, die in der Debatte um Netzneutralität eine Rolle spielten. Zu nennen ist hier insbesondere die mögliche Gefährdung der Meinungsvielfalt durch die drohende „Zersplitterung“ des Internets und den Trend zur „Appliancization“. ■



Ohne Erlaubnis grundsätzlich verboten

Datenschutzrecht verfährt nach restriktiven Grundsätzen. Dabei hat der einstige Nischenfall heute Auswirkungen auf Meinungsfreiheit, Versicherungswesen, Kreditvergaben, Medizin und Arbeitsrecht.

LORENA JAUME-PALASÍ

Das Datenschutzrecht ist ein technikbezogenes Recht. Es deckte anfangs, in den 1970er-Jahren, regulatorisch lediglich eine Nische ab. Diese betraf den Staat als Verarbeiter der Daten praktisch aller Bürger (Stichwort: Volkszählung) sowie einige wenige Großunternehmen, die sich die damals kostspielige Technik leisten konnten und eine ähnlich breit angelegte Datenverarbeitung praktizierten. Mit der technischen Entwicklung hat sich der Anwendungsbereich des Datenschutzrechts in den letzten Jahrzehnten jedoch exponentiell erweitert. Dies gilt insbesondere für den privaten Bereich, der sämtliche Unternehmen und auch Privatpersonen umfasst, sofern sie nicht rein ‚familiär' Daten verarbeiten.

Letzteres ist nach der Rechtsprechung des EuGH (Lindqvist-Entscheidung) jedenfalls bei Handlungen im öffentlichen Internet nicht der Fall. War die elektronische Datenverarbeitung früher eine Ausnahme, die den Anwendungsbereich eines speziellen Rechtsgebiets eröffnet hat, so ist sie heute die Regel in fast allen Lebensbereichen. Dementsprechend werden nahezu sämtliche Lebensbereiche und somit auch alle Politikfelder und Rechtsgebiete vom Datenschutzrecht tangiert. Das Datenschutzrecht reguliert als Querschnittsrecht direkt oder indirekt maßgeblich das Versicherungswesen, Kreditvergaben, das gesamte Internet, das Arzt-Patienten-Verhältnis und den Zugang zu Informationen (Stichwort: Recht auf Vergessen und die „Google"-Entscheidung des EuGH). Das Datenschutzrecht enthält spezielle arbeitsrechtliche Regelungen (Beschäftigtendatenschutz). Das Datenschutzrecht hat Auswirkungen auf das Äußerungs- und Presserecht, auf die Meinungsfreiheit, die unternehmerische Freiheit und die grundrechtlich geschützte Berufsfreiheit bis hin zur Kunstfreiheit.

Die Omnipräsenz des Datenschutzrechts in nahezu allen Lebensbereichen, Politikfeldern und Rechtsgebieten hat in den letzten Jahrzehnten nicht nur aufgrund der technischen Entwicklung und zunehmenden Automatisierung zugenommen. Auch die Fortentwicklung des Datenschutzrechts selbst war regelmäßig vom Ziel geprägt, etwaige Schutzlücken zu schließen. Dies geht einher mit der Annahme, dass es kein „belangloses Datum" und keine per se risikofreie Datenverarbeitung gebe. Die Datenschutzaufsichtsbehörden in Deutschland haben sich zuletzt auch für eine weitere Ausweitung des Datenschutzrechts auf den häuslichen und privaten Bereich ausgesprochen (siehe „Positionspapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. August 2015: Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung"). Mit der datenschutzrechtlichen Überwölbung anderer Regelungsmaterien entstehen auch neue Abgrenzungsfragen. Zu klären sind Fragen des Vorrangs bei gegensätzlichen Regelungszielen und die Auflösung von Wertungswidersprüchen. Die Debatten hierzu stehen vielfach erst am Anfang. Bemerkenswert in diesem Zusammenhang ist der Umstand, dass der Vollzug des Datenschutzrechts unabhängigen Aufsichtsbehörden übertragen wurde, deren ausschließliche Aufgabe die Kontrolle der Einhaltung des Datenschutzrechts ist und die – jedenfalls qua Aufgabe – nicht dazu berufen sind, andere Gesetze einzubeziehen, deren Vollzug anderen Verwaltungsbehörden übertragen wurde.

Das Datenschutzrecht hat Auswirkungen auf Äußerungs- und Presserecht,die Meinungsfreiheit, die unternehmerische Freiheit und diegrundrechtlich geschützte Berufsfreiheit bis hin zur Kunstfreiheit.

Deutschland

Das Datenschutzrecht ist in Deutschland zentral im Bundesdatenschutzgesetz (BDSG) von 1977 geregelt. In Umsetzung der EU-Datenschutz-Richtlinie 95/46 wurde es maßgeblich an europäische Vorschriften angepasst. Dennoch hat das deutsche Datenschutzrecht in mancherlei Hinsicht stets eine Sonderrolle eingenommen. Diese zeigt sich zunächst in der grundrechtlichen Fundierung des Datenschutzrechts. Das vom Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 formulierte „Recht auf informationelle Selbstbestimmung" ist in dieser Bezeichnung international kaum bekannt und hat sich begrifflich nicht durchsetzen können. Ein weiterer wesentlicher Unterschied besteht darin, dass der deutsche Gesetzgeber in Umsetzung des Volkszählungsurteils eine ganze Flut von spezifischen Datenschutzregelungen vornehmlich im öffentlichen Bereich erlassen hat, in denen der Datenverarbeitungsprozess gesetzlich beschrieben und regulatorisch untergliedert wird. Maßgebliche spezielle Begriffe des Datenschutzrechts in Deutschland sind das „Erheben", „Speichern", „Nutzen", „Verarbeiten" und „Übermitteln" von Daten. Im europäischen Recht findet sich hingegen regelmäßig nur der Oberbegriff des „Verarbeitens" von Daten. Auch im nicht öffentlichen Bereich hat der deutsche Gesetzgeber spezifische Bestimmungen erlassen. Dies gilt insbesondere für den Bereich des Beschäftigtendatenschutzes (§ 32 BDSG), der Auskunfteien (§ 28a BDSG) und des sogenannten Scoring (§ 28b BDSG), für die Markt- und Meinungsforschung (§ 30a BDSG) sowie die Videoüberwachung (§ 6b BDSG).

Das vom Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 formulierte „Recht auf informationelle Selbstbestimmung" ist in dieser Bezeichnung international kaum bekannt.

Aufgrund der europäischen Datenschutz-Grundverordnung, die am 25. Mai 2018 in Kraft tritt und unmittelbare Wirkung in den EU-Mitgliedsstaaten entfaltet, wird das Bundesdatenschutzgesetz gegenwärtig komplett überarbeitet und neu gefasst. In einem zweiten Schritt werden in der kommenden Legislaturperiode die spezifischen Datenschutzbestimmungen in zahlreichen anderen Gesetzen angepasst werden müssen. Dies betrifft unter anderem das Sozialrecht, das Arbeitsrecht sowie Steuerrecht, Aktienrecht, Grundbuchrecht und das allgemeine Zivilrecht.

Europäische Ebene

Die große datenschutzrechtliche Reform auf EU-Ebene wurde im Januar 2012 durch zwei Gesetzesinitiativen der Kommission angestoßen und im April 2016 durch die Verabschiedung der Datenschutz-Grundverordnung (EU-Verordnung 2016/679) und die EU-Richtlinie 2016/680 für den Datenschutz im Bereich Polizei und Justiz abgeschlossen. Als aktuelle

Rechtsetzungsverfahren der EU im Bereich des Datenschutzes sind die Neufassung der e-Privacy-Richtlinie sowie der aktuelle Entwurf der Richtlinie 2015/0287 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte zu erwähnen. Letzterer betrifft indirekt auch das Datenschutzrecht. Während das eigentliche Datenschutzpaket bei DG Justice angesiedelt ist, hat DG Connect die Federführung für die e-Privacy-Richtlinie und die Verhandlung der Richtlinien digitaler Inhalte.

Inhaltlich und systematisch orientiert sich die Datenschutz-Grundverordnung an dem bereits zuvor geltenden europäischen Datenschutzrecht (Richtlinie 95/46). Dieser konservative regulatorische Ansatz wurde im Laufe des Gesetzgebungsverfahrens insbesondere von Deutschland zu Beginn stark kritisiert. Die Kritik betraf den nicht öffentlichen Anwendungsbereich der Datenschutz-Grundverordnung, das heißt die Regulierung von Datenverarbeitung durch Unternehmen und Bürger. Der regulatorische Grundansatz der Datenschutz-Grundverordnung besteht darin, dass alle Datenverarbeitungen grundsätzlich verboten sind, es sei denn, sie sind aufgrund eines Erlaubnistatbestandes gestattet. Die Kombination eines regulatorischen One-Size-Fits-All-Ansatzes mit der Systematik des Verbots mit Erlaubnisvorbehalt soll dazu dienen, „Schutzlücken“ zu schließen und einen möglichst weitreichenden Anwendungsbereich zu garantieren. Begründet wurde dieser Ansatz nicht zuletzt unter Verweis auf das in der Europäischen Grundrechte-Charta (Art. 8) und in den Verträgen enthaltene Grundrecht auf Datenschutz mit einer gewissen Institutsgarantie für das einfache Datenschutzrecht (art. 16 AEUV).

Der regulatorische Grundansatz der Datenschutz-Grundverordnung besteht darin, dass alle Datenverarbeitungen grundsätzlich verboten sind, es sei denn, sie sind aufgrund eines Erlaubnistatbestandes gestattet.

Kritisiert wurde an dem konservativen Regelungsansatz, dass das One-Size-Fits-All-Verfahren auf der einen Seite Überregulierung produziere (etwa für Handwerksbetriebe oder private Internetnutzung), auf der anderen Seite jedoch unterkomplex bleibe, etwa wenn es um die Regulierung von Suchmaschinen und sozialen Netzwerken gehe. Am Verbot mit Erlaubnisvorbehalt wurde kritisiert, dass quasi als Kehrseite des Verbotsprinzips sehr allgemeine und weite Erlaubnistatbestände geschaffen würden, die teils höchst unbestimmt seien (so die Generalklausel der Datenverarbeitung „im berechtigten Interesse“ nach Art. 6 Abs. 1 f DS-GVO) und teils die Verantwortung auf den Betroffenen übertrügen (wie es bei der Einwilligung nach Art. 7 DS-GVO der Fall ist). Letztlich – so die Hauptkritik – reagiere das Datenschutzrecht nicht auf die zunehmende Vernetzung und somit die Schwierigkeiten bei der Feststellung von datenschutzrechtlichen Verantwortlichkeiten.

Marktortprinzip und Regelungen mit Drittstaaten

Wesentliche Inhalte der DS-GVO sind zudem das sogenannte Marktortprinzip und die Regelungen zum internationalen Datenverkehr mit Verarbeitern in Drittstaaten, das heißt mit Nicht-EU-Staaten beziehungsweise mit assoziierten Staaten. Das Marktortprinzip bedeutet, dass Unternehmen mit Sitz in Drittstaaten dann vollständig der Datenschutz-Grundverordnung unterworfen sind, wenn sie Waren oder Dienste in der EU anbieten. Auf diese Weise wird das EU-Datenschutzrecht automatisch ‚exportiert' sobald, ein Drittstaatsunternehmen im EU-Binnenmarkt tätig ist. Die datenschutzrechtliche Kontrolle durch die Datenschutzaufsichtsbehörden der EU und der Mitgliedsstaaten ist in den Drittstaaten, in denen sich die Unternehmen befinden, zwar eingeschränkt. Aufgrund der weitreichenden Sanktionsmöglichkeiten, die das EU-Recht bietet, ist man gleichwohl optimistisch, dass man die sogenannten Marktort-Unternehmen in Drittstaaten wirksam zur Einhaltung der EU-Datenschutzbestimmungen verpflichten kann.

Mit dem Marktortprinzip wird das EU-Datenschutzrecht automatisch ‚exportiert', sobald ein Drittstaatsunternehmen im EU-Binnenmarkt tätig ist.

Allgemein ist der Datenverkehr mit Datenverarbeitern in Drittstaaten weiterhin restriktiv geregelt und grundsätzlich nur im Hinblick auf Drittstaaten gestattet, für die ein sogenannter Angemessenheitsbeschluss der Kommission besteht. Dies ist momentan nur bei knapp einem Dutzend Drittstaaten der Fall. Besteht kein Angemessenheitsbeschluss, müssen sogenannte Binding Corporate Rules (BCR), das heißt Selbstverpflichtungen von Unternehmensgruppen, vorliegen oder Standardvertragsklauseln verwendet werden.

Eine zusätzliche Möglichkeit der Übermittlung in Drittstaaten (neben Ausnahmetatbeständen für Einzelfälle) sind sogenannte Verhaltenskodizes (Codes of Conduct). Diese sah bereits die Richtlinie 95/46 vor. In der neuen Datenschutz-Grundverordnung sind die Regelungen zu Codes of Conduct jedoch auf Betreiben Deutschlands erweitert und näher ausgestaltet worden. Die Selbstregulierungsmöglichkeiten wurden damit einerseits erweitert und andererseits stärker formalisiert (regulierte Selbstregulierung). So sehen Art. 40 und die dazugehörigen Erwägungsgründe 98 und 99 vor, dass die Codes of Conduct von Verbänden und anerkannten Normierungsorganisationen vorgelegt und maßgebliche Interessengruppen beteiligt werden. Dies ist im Sinne eines Multi-Stakeholder-Modells zu verstehen. Durch die Nutzung der Codes of Conduct für Drittstaatenübermittlung ist ein zusätzlicher Anreiz für ihre Ausarbeitung geschaffen worden. Die Codes of Conduct müssen von den Datenschutzaufsichtsbehörden genehmigt werden. Die Möglichkeiten der regulierten Selbstregulierung

könnten insbesondere im technischen Bereich genutzt werden, wo bereits Normierungsinstitutionen bestehen. Dies gilt etwa für das neu verankerte Prinzip Privacy by Design beziehungsweise Privacy by Default.

Weitere aktuelle Gesetzgebungsverfahren

Zu weiteren erwähnenswerten aktuellen Gesetzgebungsvorhaben auf der EU-Ebene zählt im Zusammenhang mit dem Datenschutz auch die Reform der sogenannten E-Privacy-Richtlinie (Directive 2002/58 on privacy and the electronic communication sector), die insbesondere Regelungen zu Cookies enthält. Daneben gibt es einen Vorschlag der Kommission zur Neufassung der Datenschutzbestimmungen für die EU-Organe sowie bezüglich der Pflichten des Europäischen Datenschutzbeauftragten (EDSB), die bisher in der Verordnung (EG) Nr. 45/2001 geregelt sind.

Internationale Ebene

Die Konvention 108 – „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" – ist eine der ersten Kodifizierungen des Datenschutzrechts auf der internationalen Ebene.

Parallel zur großen Datenschutzreform in der EU hat der Europarat eine Reform der 1981 verabschiedeten und 1985 in Kraft getretenen Datenschutz-Konvention („Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", auch bekannt als „Konvention Nr. 108") initiiert. Die Konvention 108 ist eine der ersten Kodifizierungen des Datenschutzrechts auf der internationalen Ebene. Aufgrund seiner größeren Reichweite und seiner internationalen Ausrichtung des Europarats reicht die Bedeutung weit über die Grenzen Europas und insbesondere der Europäischen Union hinaus. Die inhaltliche Zielrichtung der Reform der Konvention 108 ist ähnlich wie die der Datenschutz-Grundverordnung. Sie bleibt bei dem klassischen Regelungskonzept und ist allgemein darauf ausgerichtet, „Schutzlücken" zu schließen. Die Möglichkeiten der Mitglieder des Europarates, Ausnahmen zu erlassen, werden eingeschränkt. Dies ist auch insoweit nicht ohne Brisanz, weil die Konvention 108 – anders als Regelungen der EU – auch den Bereich der Nachrichtendienste betrifft.

Die EU spielt bei der Reform der Konvention 108 eine entscheidende Rolle. Weil die EU plant, selbst als Institution dem Europarat als Mitglied beizutreten, hat sich die Kommission von den EU-Mitgliedsstaaten ein Mandat einräumen lassen, bereits jetzt für alle EU-Mitgliedsstaaten gemeinsam die neue Konvention 108 in Straßburg zu verhandeln. Nach Auffassung der Kommission handelt diese selbst dabei in exklusivem Auftrag. Nach Auffassung der Mitgliedsstaaten hingegen ist es (weil das Thema nationale Sicherheit tangiert wird) auch den EU-Mitgliedsstaaten gestattet, neben der Kommission an den Verhandlungen teilzunehmen und selbst zu

verhandeln. Ungeachtet dieser kompetenzrechtlichen Fragen ist das Engagement der Kommission und damit der EU deshalb bemerkenswert, weil die Konvention 108 die EU im Falle ihres Beitritts zum Europarat unmittelbar binden und damit die Konvention 108 praktisch zu EU-Primärrecht werden könnte.

Noch älter als die Konvention 108 des Europarates sind die Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten („Datenschutzrichtlinien") der OECD. Sie wurden als OECD-Ratsempfehlung verabschiedet und traten am 23. September 1980 in Kraft. Die OECD-Richtlinien enthalten eine Reihe von Grundsätzen, die auch das neue Datenschutzrecht der EU prägen. Ausdrücklich nicht vorgesehen ist jedoch der One-Size-Fits-All-Ansatz. In Ziffer 3 der Richtlinien müssen Auslegungen der Datenschutz-Grundsätze möglich bleiben, die nach Kontexten der Verarbeitung und der Art der Daten unterscheiden und „personenbezogene Daten, bei denen ganz offensichtlich keine Gefahr der Verletzung der Privatsphäre und der Freiheiten von Personen gegeben ist, aus dem Anwendungsbereich dieser Richtlinien ausschließen". Aufgrund der Konvention 108 des Europarates und der Regelungen in der EU hat die Bedeutung der OECD-Richtlinien in Europa stark abgenommen. Sie besteht gleichwohl dem Grunde nach für den internationalen Datenverkehr mit sogenannten Drittstaaten und die mögliche Fortentwicklung globaler Datenschutz-Standards.

Aufgrund der Konvention 108 des Europarates und der Regelungen in der EU hat die Bedeutung der OECD-Richtlinien in Europa stark abgenommen.

Zu erwähnen ist, was diese Standards betrifft, aus jüngster Zeit vor allem das APEC Cross Border Privacy Rules (CBPR)-System. Die APEC (Asia-Pacific Economic Cooperation) ist eine Wirtschaftsgemeinschaft im Asiatisch-pazifischen Raum, die sich zum Ziel gesetzt hat, den Freihandel zu fördern. Das CBPR-System ist eine Art Zertifizierungsmodell, in dem sich Datenverarbeiter zur Einhaltung gemeinsamer Standards verpflichten. Die neue Datenschutz-Grundverordnung erkennt solche Modelle nur eingeschränkt an, da sie vornehmlich das Modell der staatenbezogenen Angemessenheitsbeschlüsse weiterverfolgt. Die USA engagieren sich (bislang) ebenfalls in der APEC und haben für das CBPR-System auch in Europa geworben. Der Datenaustausch zwischen der EU und den USA wurde indessen bislang maßgeblich durch das sogenannte Safe Harbor System geprägt, das nach der Schrems-Entscheidung des EuGH durch das sogenannte Privacy Shield abgelöst wurde.

Unter der Obama-Administration hatten sich die USA für eine „Privacy Bill of Rights" eingesetzt, die jedoch international wenig Beachtung fand. Die „Privacy Bill of Rights" hatte sich, insbesondere in der Fortschreibung,

ausdrücklich zum Ziel gesetzt, auch auf neue Phänomene wie Big Data zu reagieren. Ein wesentlicher Aspekt in der Privacy Bill of Rights war die Förderung der Selbstregulierung durch Codes of Conduct und des Multistakeholder-Modells.

Vereinte Nationen

Der UN-Menschenrechtsrat (Human Rights Council) hat 2015 einen speziellen Berichterstatter für Datenschutz eingerichtet (Special Rapporteur on Privacy). Er hat die Aufgabe, die Entwicklung und Anwendung des Datenschutzrechts weltweit zu beobachten, neue Technologien in Bezug auf ihre Gefährdungen für das Recht auf Privatsphäre zu beschreiben und dem UN-Menschenrechtsrat und der Vollversammlung der Vereinten Nationen jährlich zu berichten.

Der UN-Menschenrechtsrat (Human Rights Council) hat 2015 einen speziellen Berichterstatter für Datenschutz eingerichtet (Special Rapporteur on Privacy).

Nicht zuletzt im Zuge der Enthüllungen Edward Snowdens hat die UN-Vollversammlung bereits im Dezember 2013 eine Resolution verabschiedet, in der auf die besonderen Gefahren von heimlichen Überwachungsmaßnahmen hingewiesen wurde (Resolution 68/167).

Im November 2016 wurde eine neue Resolution on the Right to Privacy in the Digital Age vom Third Committee der Vereinten Nationen angenommen. Die Resolution nimmt neben den Gefahren einer Massenüberwachung auch den privaten Sektor in den Blick. Im Mittelpunkt steht hierbei die Bedeutung der Einwilligung der Betroffenen. Die Staaten werden aufgerufen, Datenschutzregelungen zu erlassen und durchzusetzen.

Die gleichen Ziele verfolgt die Global Network Initiative (GNI), die von einer Koalition multinationaler Unternehmen, Non-Profit-Organisationen und Universitäten getragen und unterstützt wird. Weiterhin erwähnenswert ist die Initiative des Institute of Electrical and Electronics Engineers (IEEE). Das IEEE arbeitet an technischen Standards für eine End-to-End-Verschlüsselung und an Konzepten von Privacy by Design für das Internet der Dinge. Primär geht es dabei um Definitionen und Best Practices. ■



Theoretisch nicht verantwortlich. Praktisch schon

Inwiefern sollen Internet-Intermediäre wie Suchmaschinen oder soziale Netzwerke für Urheberrechtsverletzungen haften, die Nutzer begehen? Die Debatte darüber wird (auch) in Deutschland entschieden.

JOERG HEIDRICH

Intermediäre: Das sind Dienstleister, die Kommunikation und Zugang zu Wissen und Informationen anbieten, wie Suchmaschinen, Nachrichtenaggregatoren, soziale Medien, Bewertungsportale, Websites für den Wissensaustausch oder Videoportale. Aber auch Verkaufsportale, App-Stores und Zahlungssysteme sowie Job- und Personalportale zählen zu den Intermediären. Im Normalfall sind Internet-Intermediäre nach dem deutschen Telemediengesetz für Online-Inhalte Dritter nicht verantwortlich. Die relative Freiheit von gesetzlicher Verantwortung für

Inhalte, die Intermediäre genießen, gilt als Garant für freie Meinungsäußerung. Zudem wären die Geschäftsmodelle vieler Intermediäre (Inhalte-Vermittler) unter den Bedingungen strikter Haftung für Inhalte Dritter nicht mehr praktikabel. Auch Verbraucher haben deshalb ein Interesse daran, dass für Intermediäre nicht die gleichen Vorgaben gelten wie etwa für Medienunternehmen.

Intermediäre sind Dienstleister, die Kommunikation und Zugang zu Wissen und Informationen anbieten.

Unter besonderen Voraussetzungen jedoch macht die Rechtsprechung dennoch Ansprüche gegenüber Intermediären geltend. Dies betrifft unter anderem Fälle von Urheberrechtsverletzungen. Die Meinungsfreiheit kann somit mit dem gesellschaftlichen Ziel, durch die Setzung urheberrechtlicher Anreize kreative Leistungen zu fördern, in Widerspruch geraten. Gleiches gilt für illegale Inhalte wie Kinderpornografie: Auch hier können Meinungsfreiheit und die Bekämpfung illegaler Inhalte zu entgegengesetzten Handlungsstrategien führen. Strittig ist dabei auch, mit welchen technischen Mitteln (wie etwa Websperren) die Verbreitung illegaler Inhalte verhindert werden soll. Die Aufgabe von Rechtsprechung und Politik besteht darin, zwischen den konfligierenden Werten die richtige Balance zu finden oder Wege aufzuzeigen, um konkurrierende Ansprüche gleichermaßen zu befriedigen.

Die rechtliche Situation in Deutschland

Bereits im Jahr 2000 wurde auf europäischer Ebene die E-Commerce-Richtlinie 2000/31/EG verabschiedet. Das Telemediengesetz (TMG) übersetzt die Richtlinie in nationales Recht. Das TMG, welches die Haftung im Internet maßgeblich regelt, sieht unter anderem vor, dass Zugangsdiensteanbieter „für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln", im Normalfall nicht verantwortlich sind. Auch Hosting-Provider haften für fremde Informationen, die sie für ihre Nutzer speichern, dann nicht, sofern sie von deren Rechtswidrigkeit keine Kenntnis haben und wenn sie derartige Inhalte unverzüglich löschen oder den Zugang zu ihnen sperren, sobald sie auf Rechtsverletzungen hingewiesen werden. Zudem sieht das TMG (Paragrafen 7 bis 10) auch vor, dass Intermediäre nicht verpflichtet sind, „die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen".

Richterrecht: Haftung bei Urheberrechtsverletzungen

In der Rechtspraxis hat das TMG jedoch nur eingeschränkte Gültigkeit. So entschied der Europäische Gerichtshof im Jahr 2014 in dem sogenannten

Fall „UPC Telekabel", dass Access-Providern verboten werden könne, den eigenen Kunden den Zugang zu einer Website zu ermöglichen, auf der ohne Zustimmung der Rechteinhaber urheberrechtlich geschützte Inhalte abrufbar sind. Die juristische Rechtfertigung hierfür fand das Gericht in der Urheberrechtsrichtlinie (2001/29/EG). Der Provider sei demnach als Vermittler anzusehen, dessen Dienste von dem Rechtsverletzer in Anspruch genommen werden.

Der deutsche Bundesgerichtshof folgte der Linie des EuGH mit zwei Entscheidungen aus dem Jahr 2015. Im Verfahren I ZR 174/14 verklagten mehrere Tonträgerhersteller erfolgreich die Telekom. Diese sollte den Zugriff auf die Internet-Tauschbörsen „goldesel.to" unterbinden. Nach Ansicht des Gerichts stellte nicht nur der Betrieb der Filesharing-Plattform selbst eine Rechtsverletzung dar, sondern auch die Vermittlung des Zugangs zu dieser Tauschbörse über die vom Telekommunikationsdiensteanbieter bereitgestellten Internetzugänge. Im ähnlich gelagerten Verfahren I ZR 3/1 richteten sich die Ansprüche auf Unterlassung gegen den Internetdienst 3dl.am, der mit Sammlungen von Hyperlinks den Zugang zu Kopien urheberrechtlich geschützter Werke ermöglichte. Die Kopien selbst waren bei One-Click-Hostern wie RapidShare, Netnoald oder Uploaded.to hochgeladen worden. Der BGH hatte in einem früheren Fall sogar von dem One-Click-Hoster RapidShare verlangt, dass dieser externe Internetseiten mit Linksammlungen daraufhin überprüfen müsse, ob sich dort Verweise zu entsprechenden Inhalten auf den RapidShare-Servern befinden. Diese seien dann selbstständig zu löschen (I ZR 80/12).

Als Störer gilt, wer „ohne Täter oder Teilnehmer zu sein in irgendeiner Weise willentlich und adäquat zur Verletzung eines geschützten Rechtsguts beiträgt".

In seiner Urteilsbegründung berief sich der BGH auf die sogenannte Störerhaftung. Als Störer gilt, wer „ohne Täter oder Teilnehmer zu sein in irgendeiner Weise willentlich und adäquat zur Verletzung eines geschützten Rechtsguts beiträgt". Grundsätzlich, so das Gericht, könne ein Telekommunikationsunternehmen, das Dritten den Zugang zum Internet bereitstellt, von einem Rechteinhaber als Störer in Anspruch genommen werden. Hieraus ergäbe sich auch ein Anspruch darauf, „den Zugang zu Internetseiten zu unterbinden, auf denen urheberrechtlich geschützte Werke rechtswidrig öffentlich zugänglich gemacht werden". Allerdings müsse eine solche Sperrung für das Unternehmen auch zumutbar sein.

Hassrede

Mit dem Netzwerkdurchsetzungsgesetz, das ebenfalls den Geltungsbereich des Telemediengesetzes tangiert, versucht der deutsche Gesetzgeber, die Verbreitung von strafbaren Falschaussagen oder Hassrede in

sozialen Netzwerken zu unterbinden, unter anderem durch die Androhung hoher Bußgelder bis zu 50 Millionen Euro. Der Entwurf wird von zivilgesellschaftlichen Organisationen und Unternehmensverbänden zum Teil scharf kritisiert, weil er die Meinungsäußerungsfreiheit beschränke (siehe dazu die „Deklaration für die Meinungsfreiheit"). Dies geschehe etwa dadurch, dass die Kombination der starren Löschfristen mit den bei Zuwiderhandlung anfallenden hohen Bußgeldern starke Anreize dafür setze, „ohne die erforderliche substantiierte juristische Prüfung Inhalte zu löschen" (Bitkom-Stellungnahme zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes, 2017).

Recht auf Vergessenwerden

Darüberhinaus gelten – seit dem Urteil des EuGH zum Recht auf Vergessenwerden – Intermediäre, die Informationen indexieren, als Datenverarbeiter im datenschutzrechtlichen Sinne. Aus diesem Urteil, das ursprünglich lediglich eine unmittelbare Pflicht für Intermediäre statuierte, hat die deutsche Jurisprudenz neue Abwandlungen, Fragen und Pflichten entwickelt. So entschied das Hamburger OLG, dass Online-Pressearchive eine Pflicht haben, den Zugang zu legitim veröffentlichten Meldungen im Sinne des Rechts auf Vergessenwerden einzuschränken (Urteil vom 07.07.2015, 7 U 29/12). Die Einschränkung bezieht sich auf die Bereitstellung durch Suchmaschinen: Die Archive dürfen die Meldungen nur in der Weise zum Abruf bereithalten, dass sie durch Eingabe des Namens des Betroffenen in Internet-Suchmaschinen nicht aufgefunden werden können.

Online-Pressearchive haben eine Pflicht, den Zugang zu legitim veröffentlichten Meldungen im Sinne des Rechts auf Vergessenwerden einzuschränken.

Arbeits- und Wettbewerbsrecht

Die Regulierung von Intermediären betrifft auch andere klassische politische Felder und Rechtsgebiete. So muss im Arbeitsrecht evaluiert werden, welche rechtlichen Lücken und Anpassungserfordernisse durch die Einführung von Job- und Personalportalen in die Arbeitswelt entstehen. Auch wettbewerbsrechtlich entfachte sich 2016 eine politische Diskussion über die Plattformdominanz bestimmter Anbieter, die zu einer Reform des Gesetzes gegen Wettbewerbsbeschränkungen führte. In Bezug auf die mit dem Thema der Dominanz eng verbundene Frage der Meinungsvielfalt sind ferner die Medienanstalten zu nennen. Ihnen wurde bei der Ausgestaltung neuer Bestimmungen zur Plattformregulierung im 16. Rundfunkänderungsstaatsvertrag eine wichtige Rolle zugewiesen.

Parallelfall WLAN-Haftung

Ähnliche Konflikte wie bei der Haftung von Intermediären entstehen seit vielen Jahren auch auf dem Feld der Haftung für offenes WLAN. Schon im Jahr 2010 entschied hier der Bundesgerichtshof im Rahmen der „Sommer unseres Lebens"-Entscheidung, dass ein WLAN-Betreiber für Urheberrechtsverletzungen haften kann, die über seinen Zugang begangen werden. Diese Grundsatzentscheidung wirkt in vielfältigen Ausprägungen bis heute weiter und wurde im Grundsatz auch 2016 vom Europäischen Gerichtshof bestätigt.

Nicht zuletzt auf Basis des erheblichen Drucks aus der Bevölkerung und der Industrie wurde im Juli 2016 ein erster Versuch unternommen, mehr Rechtssicherheit zu schaffen, um den Bürgern „die Nutzung von öffentlichem WLAN zu erleichtern". Im TMG, welches die Haftung im Internet regelt, wurde klargestellt, dass der dort geregelte Haftungsausschluss von Accessprovidern auch für WLAN-Betreiber gilt. Allerdings führte diese Regelung kaum zu Erfolgen. Deshalb wurde im März 2017 der Entwurf für eine erneute Neuregelung vorgestellt. Danach dürfen Rechteinhaber von dem Betreiber eines anonymen Hotspots weder Schadenersatz noch Abmahngebühren verlangen, wenn Nutzer einen Verstoß gegen Urheberrechte begehen. Allerdings fordert der Gesetzesentwurf auf der anderen Seite gleichzeitig immer noch die Einrichtung von Netzsperren durch die WLAN-Betreiber, um im Falle wiederholter Verstöße weiteren Urheberrechtsverletzungen vorzubeugen.

Schon im Jahr 2010 entschied der Bundesgerichtshof, dass ein WLAN-Betreiber für Urheberrechtsverletzungen haften kann, die über seinen Zugang begangen werden.

Multistakeholder-Prozess

Die laufenden Debatten wurden zum Initialzünder für eine offene Konsultation des Bundesministeriums für Wirtschaft, an der sich alle Stakeholdergruppen rege beteiligten. Die Konsultation wurde von Expertenworkshops flankiert, an der Vertreter der Wirtschaft, der Wissenschaft, der Zivilgesellschaft und der technischen Community beteiligt waren. Die Themenfelder der Workshops fokussierten sich auf: „Level Playing Field und Perspektiven für den Netzausbau", „Informationelle Macht – personalisierte Preissetzung in der digitalen Wirtschaft", „Individuelle Datensouveränität in der digitalen Wirtschaft", „Datensouveränität und Digitalisierung – rechtliche Rahmenbedingungen und Perspektiven" und „Transparenz in der digitalen Welt". Aus diesem Prozess entstanden ein Grünbuch und ein Weißbuch, die als Anstoß für den Entwurf einer digitalen Ordnungspolitik gelten (Weißbuch Digitale Plattformen, 2017). ■

Zwischen Hassrede und Katzenbildern

Ein Fall für die internationale Regulierung von Intermediären: Wie können in Bezug auf Internet-Inhalte, die weltweit verfügbar sind, nationale Gesetze respektiert werden?

MATTHIAS C. KETTEMANN

Der Zugang zum Internet ist die Voraussetzung, um online aktiv zu sein, zu kommunizieren oder einzukaufen. Zugang allein reicht aber nicht: Erst sogenannte Internet-Intermediäre (oder Internet-Inhalt-Vermittler) wie Google, Facebook oder Amazon ermöglichen es, das Internet zu nutzen, um über Social Media zu kommunizieren, auf Musik, Filme und Texte zuzugreifen oder überhaupt erst via Suchmaschine passende Online-Angebote ausfindig zu machen. Intermediäre verbinden Nutzer mit dem Internet, sie helfen bei der Datenverarbeitung, sie hosten und indexieren Inhalte, sie ermöglichen die Suche, sammeln Informationen, vermitteln Angebote Dritter und ermöglichen Käufe und Zahlungen.

Intermediäre tangieren in vielerlei Hinsicht Belange von gesellschaftlichem Interesse. Datenschutz und Persönlichkeitsrechte, das Recht auf freie Meinungsäußerung, die Meinungsvielfalt im öffentlichen Diskurs sowie der Schutz von Urheberrechten werden direkt oder indirekt durch das Handeln von Intermediären oder durch Vereinbarungen zwischen Intermediären und Internutzern tangiert (s. auch der Beitrag von Joerg Heidrich in diesem Band). Oft kommt es dabei zu Konflikten zwischen unvereinbaren Zielen, die immer wieder auch in Rechtsstreitigkeiten zum Ausdruck kommen. Neben diesen Zielkonflikten sind konkrete Fragen der Regulierung und Governance von Intermediären auch aus anderen Gründen von allgemeinem Interesse. Ein häufig wiederkehrendes Thema ist die Frage, inwiefern Einschränkungen des Rechts auf freie Meinungsäußerung erlaubt oder sogar geboten sind – beispielsweise, wenn es um Inhalte mit völkerrechtlich verbotenen Darstellungen geht. Diesbezügliche rechtliche Auseinandersetzungen sind zumeist auch von gesellschaftspolitischem Interesse. Eine andere Frage ist eher von perspektivischem Interesse: Wo genau ist die Grenze zwischen Medienunternehmen (die prinzipiell für Inhalte verantwortlich sind) und Intermediären (die nur begrenzt für Inhalte, die von Nutzern generiert oder eingestellt werden, verantwortlich sind) zu ziehen? Ab wann gilt ein Intermediär als Akteur, der eine medienähnliche Dienstleistung erbringt? Viele der großen Internetunternehmen produzieren eigene Inhalte und vermitteln gleichzeitig Inhalte. Wie kann zwischen ihren verschiedenen Funktionen unterschieden werden? Und schließlich: Wie soll man damit umgehen, wenn allgemeine Geschäftsbedingungen und Community Guidelines von Intermediären nationales und regionales Recht unterlaufen? Wie können in Bezug auf Internet-Inhalte, die international verfügbar sind, nationale Gesetze respektiert werden – ohne dass der Geltungsbereich dieser Gesetze dabei automatisch eine nahezu globale Ausdehnung erfährt?

Wie können in Bezug auf Internet-Inhalte, die international verfügbar sind, nationale Gesetze respektiert werden – ohne dass der Geltungsbereich dieser Gesetze dabei automatisch eine nahezu globale Ausdehnung erfährt?

Rechte und Freiheiten sichern: Der Staat ist in der Pflicht

Staaten sind dazu verpflichtet, die Rechte und Freiheiten ihrer Bürger auch gegen Intermediäre durchzusetzen. Dies erschöpft sich nicht in der Anregung von Selbstkontrollmechanismen. Auf der anderen Seite sind staatlichem Handeln durch völkerrechtliche und andere Vereinbarungen



Hassrede im Netz und ihre Konsequenzen

„Dieses Pack gehört gesteinigt und an die Wand gestellt. Allen voran diese erbärmliche Drecksau von OB Jung, dieser Voll-Assi."

Konsequenz: 1.380 Euro Strafe

„Ich bin dafür, dass wir die Gaskammern wieder öffnen und die ganze Brut da reinstecken."

Konsequenz: 4.800 Euro Strafe

„Sogesehen haben die Juden am Holocaust des 2. Weltkrieges auch selber schuld. Vor allem die im Warschauer Ghetto..."

Konsequenz: 5.000 Euro Strafe

„Merkel muss öffentlich gesteinigt werden."

Konsequenz: 2.000 Euro Strafe

Nachdem die Stiftung Warentest darauf aufmerksam gemacht hatte, wie man Anzeige gegen Personen erstatten kann, die im Internet strafbare Äußerungen verbreiten („Hassrede"), listete sie in einem späteren Beitrag ergangene Strafen auf.

https://www.facebook.com/stiftungwarentest/photos/a.10150147181713332.346613.128592903331/10154838513143332/?type=3&theater

aber auch Grenzen gesetzt, was Eingriffe in den Verfügungsbereich von Internet-Intermediären und somit in die Meinungsfreiheit betrifft. Die Sperrung von Online-Angeboten durch staatliche Instanzen ist nur begrenzt zulässig.

Die Diskussion um die rechtlichen Verpflichtungen von Intermediären hat eine lange Geschichte. Den UN Guiding Principles on Business and Human Rights folgend haben Intermediäre eigenständige Pflichten, Menschenrechte zu respektieren, eine „corporate responsibility to protect", die unabhängig von der staatlichen Pflicht ist, Menschenrechte zu sichern. Unternehmen kommen diesen Pflichten etwa durch Transparenzberichte, verstärkter Kontrolle von Subunternehmen entlang der Lieferkette und Human Rights Impact Assessments nach. Es bestehen auch einige Initiativen von Technologieunternehmen, wie die Global Network Initiative, in denen sie sich zu selbst entwickelten Prinzipien bekennen (die allerdings menschenrechtlich grundiert sind) und im Rahmen eines *Accountability, Policy & Learning Framework* ihre Performance verbessern wollen. Doch dies geht vielen Staaten und Nutzern nicht weit genug.

Auf globaler Ebene sind Intermediäre äußerst mächtige Player geworden. Die Nutzerzahlen vieler sozialer Netzwerke machen sie (auch wenn der Vergleich mit Einwohnerzahlen hinkt) zu größeren Entitäten als viele Staaten. Gleichzeitig stehen Unternehmen unter einem doppelten Druck: Nutzer wollen sich sicher und unterhalten fühlen, und Staaten wollen, dass ihre Rechtssysteme anerkannt und eingehalten werden. Schon dies setzt Intermediäre dem Problem aus, für (fast) jeden Staat eigene Angebote schalten zu müssen. Google kämpft seit 2016 mit der französischen Datenschutzbehörde CNIL und den Ansprüchen französischer Richter, das Recht auf Vergessen global umzusetzen (was einem Oktroi einer französischen Entscheidung auf die Suchfunktionalität weltweit gleichkäme). Facebook

wird verklagt, weil es nach Upload eines impressionistischen Bildes eines weiblichen Unterleibs den Account eines französischen Users gesperrt hatte („French Court rules Against Facebook in Gustave Courbet Lawsuit").

EGMR-Entscheide liefern Kriterien für die Löschung von Inhalten

Die Wahrung von Datenschutz und Persönlichkeitsrechten, der Respekt von völkerrechtlichen Vereinbarungen (etwa dem Verbot von gewaltverherrlichender Hassrede oder sexueller Ausbeutung von Minderjährigen) sowie der Schutz der Urheberrechts erfordern es, dass Intermediäre dazu verpflichtet werden, unter bestimmten Umständen Internet-Inhalte zu löschen.

In einigen Fällen – wie bei der Verletzung des Urheberrechtes – geschieht dies nach Aufforderung durch Betroffene („notice and take down"). In anderen Fällen ist von Intermediären aber auch Eigeninitiative gefragt, um der Verbreitung illegaler Inhalte entgegenzusteuern. Hier obliegt es den Intermediären selbst, zwischen Rechten abzuwägen. Das Dilemma: Löschen sie zu viel, wird ihnen vorgeworfen, auf unrechtmäßige Weise die Meinungsfreiheit im Netz zu beschneiden. Nutzer wandern ab. Löschen sie zu wenig, beschuldigt man sie beispielsweise zu wenig gegen Hassrede zu unternehmen. Eine Orientierung in dieser Situation bieten vergangene Entscheidungen des EGMR.

Zunächst ist festzuhalten, dass der EGMR grundsätzlich der Meinungsäußerungsfreiheit einen sehr hohen Stellenwert einräumt und selbst Meinungen schützt, die „offend, shock or disturb". In den Fällen *Yildirim v. Turkey* (case no. 3111/10) und *Cengiz and Others v. Turkey* hat der EGMR festgehalten: Ein Staat, der ohne legitimen Grund den Zugang zu Intermediären verunmöglicht, verletzt die Rechte und Freiheiten, die in der Europäischen Menschenrechtskonvention garantiert werden.

Das Menschenrechtshochkommissariat betont in seinem Bericht „The Right to Privacy in the Digital Age": Das Recht auf Privatleben und der Datenschutz sind gerade im Internet von besonderer Bedeutung.

Hinsichtlich des Rechts auf Meinungsäußerungsfreiheit gibt es mehr oder weniger klare Grenzen. Diese betreffen zum einen die Wahrung der Privatsphäre. Denn wie das Menschenrechtshochkommissariat in seinem Bericht „The Right to Privacy in the Digital Age" betont, ist das Recht auf Privatleben und der Datenschutz gerade im Internet von besonderer Bedeutung. Details dazu wurden in den EuGH-Urteilen

Schrems v. Data Protection Commissioner ausgearbeitet („Schrems I" und „Schrems II"; siehe auch „Human rights guidelines for Internet service providers").

Auf der anderen Seite stößt die Meinungsäußerungsfreiheit bei völkerrechtlich verbotenen Äußerungen und Darstellungen an klare Grenzen. Darunter fallen Aufforderungen zum Genozid, Terrorismus, qualifizierte Diskriminierung in Form von gewaltverherrlichender Hassrede und sexuelle Ausbeutung von Minderjährigen. Hier sind Intermediäre in der Pflicht, von sich aus mit der Löschung entsprechender Inhalte aktiv zu werden.

Wer muss haften – unter welchen Umständen?

Eine Frage ist es, anhand welcher Kriterien legale von illegalen Inhalten unterschieden werden sollen. Eine andere Frage ist, wer im konkreten Fall eine Lösung vornehmen oder vielleicht sogar Schadensersatz leisten muss und wann ein Akteur für illegale Inhalte rechtlich verantwortlich ist. Hierzu zählt auch die Frage, unter welchen Umständen Intermediäre eigenständig aktiv werden, oder ob sie nur auf Löschungsaufforderungen reagieren müssen.

Grundsätzlich bietet Artikel 14 der E-Commerce-Richtlinie einen starken Schutz für Dienste der Informationsgesellschaft, über deren Plattformen Nutzer Inhalte öffentlich zugänglich machen. Mitgliedsstaaten können einen Anbieter nur für Inhalte verantwortlich machen, die dieser der im Nutzerauftrag gespeichert hat, wenn er „tatsächlich Kenntnis von der rechtswidrigen Tätigkeit oder Information [hat] und, in Bezug auf Schadenersatzansprüche, […] er sich […] Tatsachen oder Umstände[n] bewusst [ist], aus denen die rechtswidrige Tätigkeit oder Information offensichtlich ist". Eine allgemeine „Recherchepflicht" oder Vorabzensur wäre aber (Artikel 15 Abs 1 E-Commerce-RL und mehreren Urteienl des EuGH zufolge) europarechtswidrig. In *Delfi v. Estonia* entschied die Große Kammer, dass mit Blick auf die Rechte und Interessen anderer und auf die Gesellschaft als Ganze den Vertragsstaaten erlaubt sei, unter bestimmten Bedingungen Intermediäre (hier: ein Internet-Newsportal) in die Haftung zu nehmen. Zu diesen Bedingungen zähle, dass es sich um ein kommerzielles Newsportal handle; dass das Unternehmen Kommentare, die „klar an sich schon rechtswidrige" Hassrede darstellten und zu Gewalt aufriefen, nicht unverzüglich (das heißt bis zu sechs Wochen nach deren Veröffentlichung) nach

Grundsätzlich bietet Artikel 14 der E-Commerce-Richtlinie einen starken Schutz für Dienste der Informationsgesellschaft, über deren Plattformen Nutzer Inhalte öffentlich zugänglich machen.

deren Veröffentlichung entfernt habe; dass das Portal den Autoren erlaubt habe, anonym zu bleiben; und dass der Schadenersatz nur gering sei (320 Euro). Von einer Pflicht zur „Privatzensur" distanzierte sich der EGMR. Aber dennoch hatten Straßburgs Intermediäre die Rolle, zu bewerten, ob ein Posting nur beleidigend ist (dann kann auf eine „notice" gewartet werden) oder „an sich" schon rechtswidrig ist (dann ist dieses gleich zu löschen).

In *MTE and Index.hu ZRT v. Hungary (2016)* bestätigte der EGMR seinen Ansatz und betonte, dass Notice-and-takedown-Verfahren weiterhin legitim seien, solange die Kommentare nicht an sich klar rechtswidrig seien. In *Rolf Anders Daniel Pihl v. Sweden* (2017) bekräftigte Straßburg einmal mehr, dass die Art der Äußerung; der Kontext; die Größe und kommerzielle Natur der Plattform; ihre Verfahren zur Entfernung inkriminierter Kommentare; die Geschwindigkeit der Reaktion; die Möglichkeit der direkten Haftung des eigentlichen Autors und die (finanziellen) Folgen der nationalen Entscheidung für die Plattform relevant für die Entscheidung der Frage seien, ob ein Menschenrecht verletzt worden sei.

Politische und gesellschaftliche Fragen

Die Weiterentwicklung des rechtlichen Rahmens für Intermediäre vor dem Hintergrund neuer technologischer Entwicklungen, innovativer Geschäftsmodelle und durch Gerichtsentscheide erfolgter Klarstellungen und Interpretationen geltender Gesetze ist eine wichtige politische Aufgabe.

Generell treffen hier Recht und allgemeine Geschäftsbedingungen konfliktreich aufeinander. Perspektivisch wird die Politik die Frage stellen müssen, wie lange erfolgreiche soziale Netzwerke noch rein ‚private Räume' bleiben und ab wann sie als (zumindest) quasi-öffentliche Räume gesehen werden müssen. Ein Kriterium für die Definition dieser Grenze kann man aus der Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) im Fall *Appleby and Others v. United Kingdom* ableiten. In diesem Fall hatten politische Aktivisten dagegen geklagt, dass der Betreiber einer Shopping Mall es ihnen verwehrte, Flugblätter mit Unterschriftenlisten im Eingangsbereich und in der Wandelhalle der Mall zu verteilen. Die Richter wehrten die Ansprüche der Aktivisten ab. Die Begründung: Die Aktivisten hätten für ihr Anliegen auch in den Geschäftsstraßen der Altstadt werben oder über lokale Medien kommunizieren können. Umgekehrt folgt aus dieser Urteilsbegründung: Wenn ein für das Gemeinwesen wichtiger Diskurs außerhalb von privat konstituierten Räumen tatsächlich nicht mehr erfolgreich stattfinden kann, können staatliche Eingriffe in den Verfügungsbereich von privaten Akteuren (sei es eine Shopping Mall oder eine von einem

Internet-Intermediär betriebene Kommunikationsplattform) durchaus legitim sein. Im vorliegenden Fall hätte der staatliche Eingriff darin bestanden, dass dem Mall-Betreiber auferlegt worden wäre, das Verteilen von Flugblättern zu gestatten. Ähnlich argumentierten die Richter des deutschen Bundesverfassungsgerichts in der „Fraport Entscheidung". Hier ging es um die Frage, inwiefern Meinungskundgebungen und Demonstrationen auf dem Gelände des Flughafens Frankfurt von der Betreibergesellschaft verboten werden können. Ein zentraler Begriff in der Urteilsbegründung ist



Die Organisation European Digital Rights (EDRi) versuchte mit einer Kampagne, Nutzer dazu zu bewegen, sich an der Konsultation der EU zur Rolle und Regulierung der Internet-Plattformen und Intermediäre zu beteiligen.

https://edri.org/wp-content/uploads/2015/12/Eurpean_Commissions_Platform_Consultation.png

der des „öffentlichen Forums", welches dadurch charakterisiert ist, „dass auf ihm eine Vielzahl von verschiedenen Tätigkeiten und Anliegen verfolgt werden kann und hierdurch ein vielseitiges und offenes Kommunikationsgeflecht entsteht". Aus einem solchen öffentlichen Forum, so die Karlsruher Richter, könne die „politische Auseinandersetzung in Form von kollektiven Meinungskundgaben durch Versammlungen nicht herausgehalten werden".

Eine weiteres, eher praktisches Thema für die Politik ist der sich nicht immer unproblematisch gestaltende Rechtsvollzug. Bei gemeldeten, nach dem Recht mancher Staaten strafbaren Äußerungen (etwa Leugnung des Holocausts) sind Intermediäre zu oft nicht in der Lage (oder willens), effektiv Löschungen vorzunehmen. Zwar haben sich wichtige soziale Netzwerke in einer Task Force 2015 darauf geeinigt, binnen 24 Stunden nach deutschem Recht strafbare Inhalte zu löschen („Together against Hate Speech"). Jedoch werden einem Bericht von jugendschutz.net zufolge bei Twitter nur ein Prozent und bei Facebook nur 39 Prozent der inkriminierten Inhalte rechtzeitig gelöscht (bei YouTube hingegen 90 Prozent). Überraschend ist dies insofern, als Intermediäre bei der Bekämpfung von Urheberrechtsverletzungen unter Beweis stellen, dass das Löschen illegaler Inhalte vergleichs-

weise problemlos möglich ist. So bieten einige Intermediäre Copyright-Inhabern bevorzugten Zugang zu Plattformen, um geschützte Inhalte zu identifizieren. Löschanforderungen, die Copyright-Verletzungen betreffen, kommen Intermediäre regelmäßig viel schneller nach als geflaggter Hassrede. Hier ist (auch) politische Initiative gefragt.

Ein weiteres Problemfeld: Einzelne Intermediäre, wie etwa Google oder Facebook, nehmen eine sehr zentrale Position ein, was die Verfügbarmachung von Inhalten betrifft. Dies könnte die Sicherung von Meinungsvielfalt und die Begrenzung von Meinungsmacht infrage stellen. Auch die Art und Weise, wie Intermediäre bestimmte Inhalte priorisieren, ist davon betroffen, beispielsweise die durch Algorithmen gesteuerte und individualisierte Steuerung von Medieninhalten. Oftmals werden in diesem Kontext Forderungen nach Transparenz von algorithmenbasierten Entscheidungen erhoben sowie nach Schutz vor Diskriminierung durch Algorithmen. Ein ebenfalls in diesem Kontext diskutiertes Phänomen ist die sogenannte „Filter Bubble“: Medienkritiker befürchten, dass der Konsum von zunehmend personalisierten Nachrichten und Inhalten dazu führt, dass eine allgemeine und übergreifende Medienöffentlichkeit signifikant an Bedeutung verlieren und die demokratische Gesellschaft dadurch Schaden erleiden könnte.

Einher mit der Sorge um Konzentration von Meinungsmacht geht die Forderung nach Datenportabilität. Datenportabilität ist ein Gegengewicht zu dem in Netzwerk-Ökonomien zu beobachtenden Trend des Lock-in: Kunden und Nutzer insbesondere von Social-Media-Plattformen ist es oft nahezu unmöglich, zu einem anderen Anbieter zu wechseln, weil einerseits ein Großteil der Kommunikationsbeziehungen exklusiv an den bestehenden Anbieter gebunden ist, andererseits auch vom Nutzer selbst oftmals über viele Jahre hinweg erzeugte Inhalte bei dem bestehenden Anbieter liegen. Datenportabilität würde es Nutzern ermöglichen, ihre selbst generierten Informationen von einer Plattform auf eine andere umzuziehen. Die Möglichkeit eines solchen Umzuges wiederum würde der Meinungsmacht von Intermediären Grenzen setzen: Nutzer, die mit den Geschäftsbedingungen eines Intermediärs nicht mehr einverstanden sind, könnten einfach den Anbieter wechseln. Die Portabilität von Inhalten zwischen konkurrierenden Intermediären und die Kontrolle von Nutzern über seine gespeicherten Daten sind zentrale Fragen der nächsten Jahre. Die EU hat sich bislang lediglich der Portabilität von Onlinedienstleistungen (wie Filmen und E-Books) zwischen Mit-

Löschanforderungen, die Copyright-Verletzungen betreffen, kommen Intermediäre regelmäßig viel schneller nach als geflaggter Hassrede. Hier ist (auch) politische Initiative gefragt.

gliedsstaaten angenommen. Ein Recht auf Portabilität von eigenen Daten existiert (noch) nicht. Es zu konturieren wäre auch nicht einfach, da der Versuch einen Eingriff in die unternehmerische Freiheit der Intermediäre darstellen würde. Weitere Schwierigkeiten hängen mit der Natur von sozialen Medien zusammen. Bei (aufeinander folgenden) Kommentaren in einem Diskussionsforum zum Beispiel würde der Transfer eines aus dem Kontext gerissenen einzelnen Kommentars wenig zielführend sein. Auch würden kleinere Anbieter durch Anforderungen an Datenportabilität, die mit hohem technischem Aufwand einhergehen, im Wettbewerb deutlich benachteiligt werden.

Agenten der Veränderung

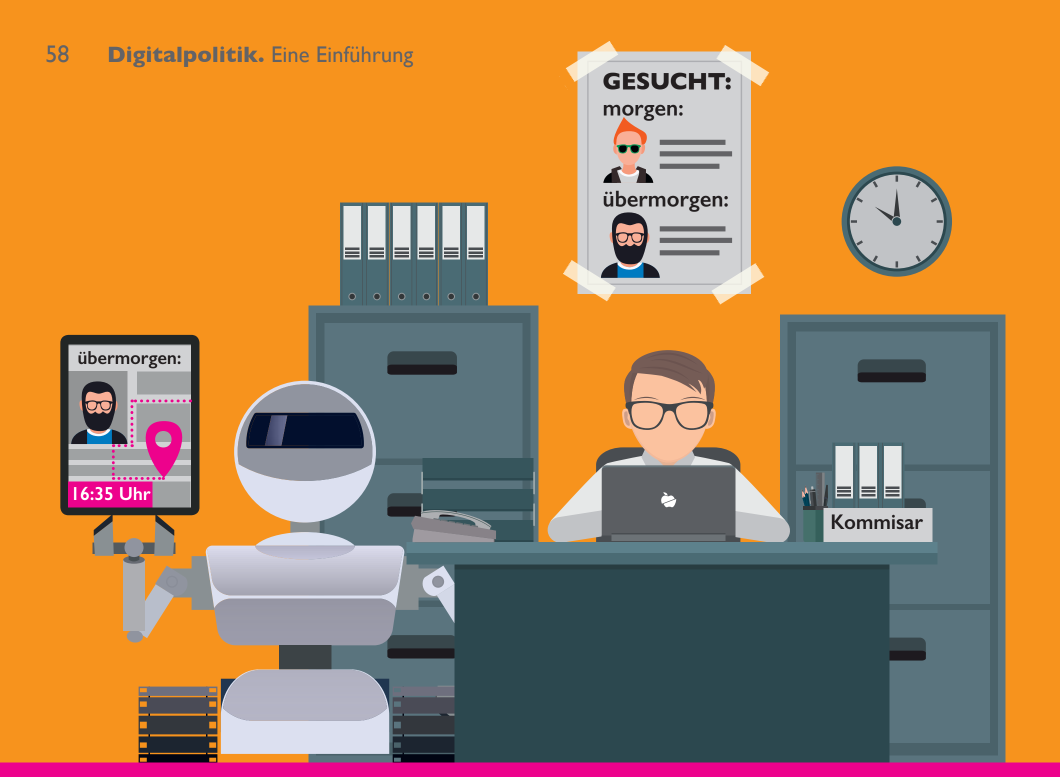
International haben sowohl die UNESCO („Fostering Freedom Online") als auch die OECD („The Economic and Social Role of Internet Intermediaries") wegweisende Berichte zu Intermediären und deren Bedeutung für die Entwicklung des Internets beziehungsweise für die Online-Freiheit in Auftrag gegeben. Auf EU-Ebene ist die derzeit in der Diskussion befindliche EU-Richtlinie über die Bereitstellung digitaler Inhalte zu erwähnen, die den Vertrieb digitaler Medien durch Intermediäre wie etwa Apple oder Amazon betrifft. Sehr intensiv in die Diskussion um Intermediäre eingebracht hat sich auch der Europarat, der bis Ende 2017 eine Empfehlung des Ministerkomitees zu Internet-Intermediären veröffentlichen wird. In dieser werden Staaten daran erinnert, die Rechte ihrer Bürger online zu schützen. Mit dem Netzwerkdurchsetzungsgesetz versucht beispielsweise der deutsche Gesetzgeber, die Verbreitung von strafbaren Falschaussagen oder Hassrede in sozialen Netzwerken zu unterbinden.

Transnationale Unternehmen sind sich zunehmend ihrer besonderen Stellung bewusst. In Initiativen wie der Global Network Initiative bekennen sie sich zu zentralen Rechten und Werten, die auch ihr Verhalten als Intermediäre beeinflussen sollten.

Die EU Kommission hat im Herbst 2015 im Zusammenhang mit dem Aufkommen der partizipativen Wirtschaft eine offene Konsultation für Onlineplattformen initiiert. Erbeten wurden Meinungen zur Rolle der Plattformen in der partizipativen Wirtschaft und in Bezug auf Rechte und Haftungsfragen, vorhandene Anbieter, Innovationspotenziale und Wahlmöglichkeiten der Verbraucher. Die Konsultation wurde im Zuge der Strategie für den digitalen Binnenmarkt gestartet. Das Ergebnis dieser Konsultation, an der sich alle Stakeholder Gruppen beteiligten, soll als Grundlage für weitere Arbeiten

an einem europäischen Konzept für die partizipative Wirtschaft dienen und fließt unter anderem in die Konkretisierung der EU-Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte.

Transnationale Unternehmen sind sich zunehmend ihrer besonderen Stellung bewusst. In Initiativen wie der Global Network Initiative bekennen sie sich zu zentralen Rechten und Werten, die auch ihr Verhalten als Intermediäre beeinflussen sollten. Zivilgesellschaftliche Organisationen und die Wissenschaft haben versucht, zumindest im Bereich der Intermediärshaftung menschenrechtssensible Leitlinien vorzuschlagen: die Manila Principles. Ein Nebenaspekt: Die Tatsache, dass die Manila Principles durch das internationale Diskussionsforum RightsCon entwickelt wurden, macht zugleich deutlich, inwiefern informelle Foren durchaus wahrnehmbaren (auch normativen) Einfluss haben können. Zu diesen gehört auch die Dynamic Coalition on Platform Responsibility (CD PR) des Internet Governance Forum. ■



Von Autopilot bis Predictive Policing

Algorithmen, Big Data, KI und Robotik: Automatisierte Entscheidungsfindung wird bereits heute in nahezu allen Bereichen eingesetzt. Dennoch steht die Technologie erst an ihrem Anfang.

LORENA JAUME-PALASÍ UND MATTHIAS SPIELKAMP

Automatisierte Entscheidungsprozesse (automated decision-making, ADM), die von Algorithmen gesteuert werden und auf der Auswertung großer Datenmengen (Big Data) beruhen, nehmen bereits heute breiten Raum in unserer Gesellschaft ein. Sie reichen von Fahrerassistenz-Systemen, die Autos bei Gefahr abbremsen, bis hin zu Scoring-Mechanismen, die darüber entscheiden, ob Menschen ein Kredit gewährt wird. Auch staatliches Handeln wird immer öfter von ADM-Systemen unterstützt, sei es in der „vorausschauenden Polizeiarbeit“

(predictive policing) oder bei der Entscheidung darüber, ob jemand am Flughafen besonders streng kontrolliert wird. Diese Entwicklung steht gerade erst an ihrem Anfang; in wenigen Jahren werden alle Bürgerinnen und Bürger täglich auf die eine oder andere Art von Entscheidungen dieser Systeme betroffen sein.

Traditionell werden die Felder Big Data auf der einen Seite und Algorithmen, künstliche Intelligenz und Robotik auf der anderen Seite in der politischen Diskussion getrennt voneinander behandelt. Jedoch ist eine Analyse der Funktionsweise von Algorithmen nicht möglich, ohne auch die Daten zu thematisieren, die von einem Algorithmus verarbeitet werden. Vor allem bei komplexeren, lernenden Algorithmen prägen die Daten die Lernrichtung des Algorithmus mit. Algorithmen sind an sich lediglich schlanke Handlungsanweisungen: Derselbe Algorithmus, der dafür genutzt wird, Filme vorzuschlagen, kann auch für die Krebsforschung verwendet werden. Die dafür genutzten Daten und der Kontext machen den Unterschied. Daher ist es für die Beurteilung, wie wirksam und effizient ein Algorithmus ist und welchen Mehrwert er bietet, unabdingbar, ihn in Kombination mit der Datenbank zu betrachten.

Schon jetzt werden Automatisierungsprozesse in nahezu allen Lebensbereichen eingesetzt und betreffen daher viele politischen Handlungsfelder:

- Wirtschaft und Finanzen (Handel mit Waren, Dienstleistungen und Aktien)
- Rechtsfindung, -anwendung, -zugang und -verwaltung (Legal Tech)
- Gesundheit (Robotik im Operationssaal, in der Altenpflege und Diagnostik)
- Arbeitswelt (Industrieroboter, Automatisierungsprozesse in Personalauswahl und -management, Crowdworking-Plattformen wie Uber, Airbnb u.a.)
- öffentliche Hand (Grenzkontrolle, Steuerbescheide, Verwaltung, Sicherheit)
- Verkehr (automatisiertes und autonomes Fahren, Autopiloten im Flugzeug, Verkehrssteuerung, Logistikplanung)
- Bildung (Leistungsbeurteilung)
- Forschung (alle Arten von komplexen Modellierungen, z.B. in der Klimaforschung)
- Verbraucherschutz (Spielroboter, Roboter zum Staubsaugen und Rasenmähen, persönliche Assistenten wie Alexa, Siri u.a., Sexroboter)

Fast immer handelt es sich bei Automatisierungsprozessen um relativ komplexe Verfahren. Selten kann die Lenkung des Verfahrens und die Verantwortung dafür einer einzelnen Stelle zugeordnet werden.

Die Lage in Deutschland

Die Debatte um Automatisierung hat im Laufe des Jahres 2016 an Fahrt aufgenommen. So hat das Bundesministerium für Verkehr und digitale Infrastruktur eine Ethikkommission zum automatisierten Fahren einberufen; Anfang 2017 wurde der Gesetzentwurf zum automatisierten Fahren vom Bundeskabinett verabschiedet. Eine Harmonisierung des EU-Verkehrsrechts wird zudem von großen deutschen Konzernen gefordert, die auch autonom fahrende Lkws mit dem sogenannten Platooning-System entwickeln und bereits in Pilotprojekten erproben. In diesem Rahmen ist die Debatte um die Idee eines Datenpasses und eine mögliche Verrechtlichung des Begriffes „Dateneigentum" zu sehen, mit dem ein Ausschließlichkeitsrecht der Unternehmen verankert werden soll. Dadurch sollen auf Algorithmen basierte Dienstleistungen und Anwendungen optimiert und abgesichert werden.

Eine Harmonisierung des EU-Verkehrsrechts wird von großen deutschen Konzernen gefordert, die auch autonom fahrende Lkws mit dem sogenannten Platooning-System entwickeln und bereits in Pilotprojekten erproben.

Das Bundesfinanzministerium hat 2016 eine Studie zum FinTech-Markt in Deutschland vorgelegt und im März 2017 den FinTechRat gegründet, der das Ministerium zu „Fragen der digitalen Finanztechnologie, insbesondere zu (informations-)technologischen Entwicklungen, ihren Potenzialen sowie zu Chancen und Risiken" beraten soll. Die Studie fokussiert auf die Segmente Finanzierung und Vermögensmanagement. Zu den FinTech-Unternehmen zählen unter anderem Internetportale für „Robo Advice", also Portfoliomanagementsysteme, „die algorithmusbasiert und in der Regel mit einem hohen Grad an Automatisierung Anlageempfehlungen geben und teilweise auch Anlageentscheidungen treffen". Mit mehr als einer Verzehnfachung des Marktvolumens verzeichnete das Segment Robo Advice eine beachtliche durchschnittliche jährliche Wachstumsrate.

Auch das Bundesministerium für Wirtschaft hat sich im Rahmen einer offenen, nach dem Multistakeholder-Modell ablaufenden Konsultation mit Fragen von Algorithmen und Nutzungsrechten (Dateneigentum) beschäftigt sowie mit der Marktmacht digitaler Plattformen (Wettbewerbsrecht), die sich algorithmischer Prozesse bedienen. Die Ergebnisse dieser

Konsultation wurden in einem Grünbuch und einem Weißbuch zu digitalen Plattformen zusammengefasst (vgl. den Beitrag von Joerg Heidrich zu Intermediären in Deutschland).

Die Fragen des Dateneigentums und des Wettbewerbsrechts werden derzeit von mehreren Bundesbehörden aus regulatorischer Sicht evaluiert. Zur Diskussion stehen vor allem drei Ideen:

- gesetzliche Ausschließlichkeitsrechte an Daten zu schaffen oder zu stärken („Eigentum an Daten")
- mithilfe von Verträgen die Rechte an Daten zu klären
- eine Stärkung der Datenzugangsrechte (Auskunftsrecht, Datenportabilität)

Auch die ethische Dimension der technologischen Entwicklung wird diskutiert. Ein Problem: Durch den Einsatz von ADM-Systemen kann sich die Nachvollziehbarkeit von Entscheidungen verschlechtern. Plädiert wird unter anderem dafür, dass offengelegt werden muss, wenn selbstlernende Algorithmen eingesetzt werden, um die Transparenz und Prüfbarkeit automatisierter Entscheidungen zu erhöhen, und dass sich in relevanten Fällen betroffene Unternehmen dazu verpflichten, ethische Standards einzuhalten.

Das Bundesministerium für Bildung und Forschung (BMBF) hat bereits 2014 das Berlin Big Data Center und das Competence Center for Scalable Data Services in Dresden aufgebaut. Die geförderte Forschung konzentriert sich auf Big Data in der industriellen Produktion, aber auch in den Lebens- und Geowissenschaften. Fragen des Datenschutzes, der Privatheit und der IT-Sicherheit begleiten die Vorhaben.

Das Bundesinnenministerium beschäftigt sich mit Fragen der automatisierten Entscheidungsfindung und Datennutzung im Rahmen der Anpassung der Datenschutz-Grundverordnung an nationales Recht. Dafür wurde eigens das neue Themenfeld „Datenpolitik" geschaffen; erste öffentliche Multistakeholder-Expertenrunden zu Algorithmen und Automatisierung haben bereits stattgefunden. Darüber hinaus werden bei der Auswertung von Fluggastdaten (Passenger Name Records, PNR) zur Verfolgung terroristischer Anschläge Algorithmen eine Rolle spielen.

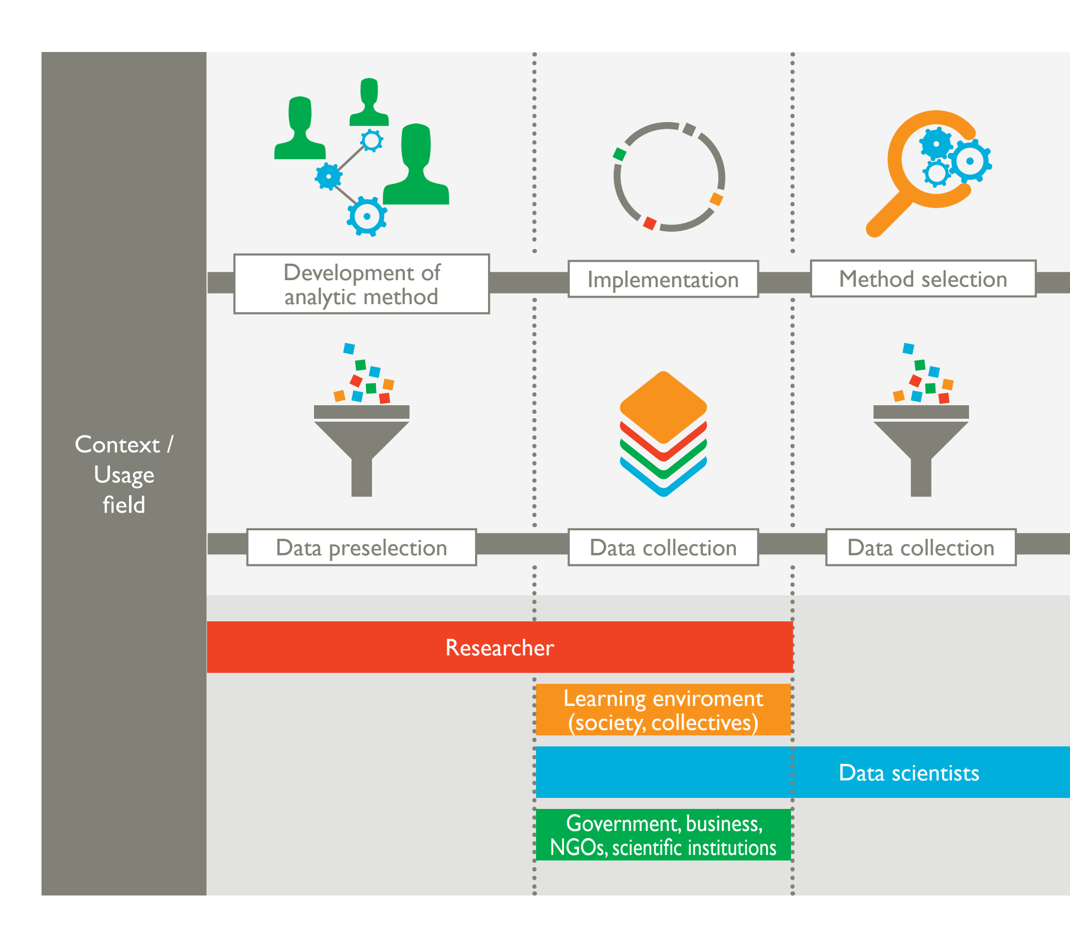
Auch die Polizei bedient sich automatisierter Verfahren beim Einsatz der sogenannten vorausschauenden Polizeiarbeit (predictive policing), um Eigentumsdelikte zu verhindern. In Bayern, Berlin, Hessen, Niedersachsen und Nordrhein-Westfalen sind derartige Systeme bereits im Einsatz, zum

Teil in Probebetrieb. In Baden-Württemberg, Hamburg und Brandenburg gab oder gibt es Modellversuche und Machbarkeitsstudien.

Europäische Ebene

Auf europäischer Ebene verlaufen politische Diskussionen um die Automatisierung geteilt in zwei verschiedene Hauptthemen: Algorithmen und Robotik.

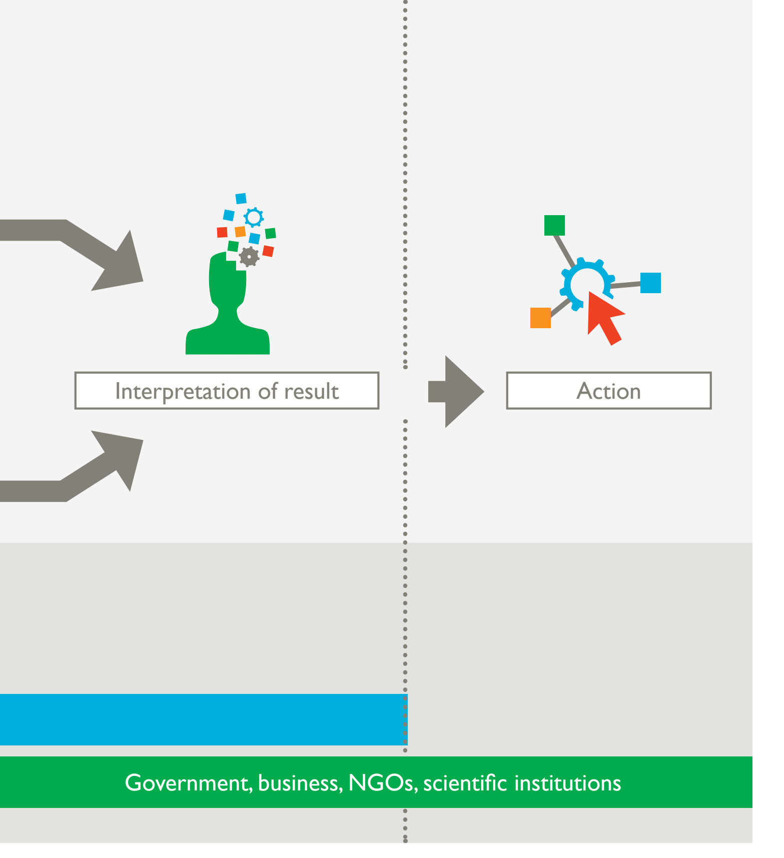
In der EU können Algorithmen nicht patentiert werden: „Programme für Datenverarbeitungsanlagen" sind nach Artikel 52(2) des Europäischen Patentübereinkommens (EPÜ) von der Patentierung ausgeschlossen. Mit der EU-Verordnung zur europäischen Normung (1025/2012) wurden politische Rahmenbedingungen und Rechtsgrundlagen für die Standardi-



sierung innerhalb der EU geschaffen. Die drei anerkannten europäischen Normungssysteme, das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) und das Europäische Institut für Telekommunikationsnormen (ETSI), haben zu diesem Zweck die „Europäische Normungsstrategie 2020" entwickelt, um die Entwicklung von Standards voranzutreiben. Insbesondere die CEN besteht aus Experten aller Stakeholder-Gruppen (Industrieverbände, Konsumenten, aber auch andere Interessengruppen). Die dort entwickelten Normen haben zwar keinen bindenden Charakter; da alle drei Institutionen jedoch von der EU als Standardisierungsorgane anerkannt werden, haben diese Normen Gewicht.

Derzeit wird auch eine mögliche Regulierung von Robotern diskutiert; zur Analyse des Regulierungsbedarfs bei Algorithmen laufen derzeit

Derzeit wird auch eine mögliche Regulierung von Robotern diskutiert; zur Analyse des Regulierungsbedarfs bei Algorithmen laufen derzeit Konsultationen.



Von der Konzeption über die Entwicklung bis zur Anwendung von Systemen zur automatisierten Entscheidungsfindung sind verschiedene Akteure beteiligt. Sie alle haben Einfluss auf die Ergebnisse und tragen somit auch einen Teil der Verantwortung.

Quelle: algorithmwatch.org

Konsultationen. Ende 2016 präsentierte die EU-Abgeordnete Mady Delvaux einen Bericht mit Empfehlungen an die EU-Kommission, um ein Gesetzgebungsverfahren zur zivilrechtlichen Regulierung von Robotern anzustoßen. Vorgeschlagen wird die Gründung einer Europäischen Agentur; außerdem rechtliche Regelungen zu Fragen der Haftung, des geistigen Eigentums und des Datenflusses sowie der Standardisierung und Sicherheit von autonomen Fahrzeugen, von Drohnen, Pflegerobotern, medizinischen Robotern und Robotern für die „Reparatur und Optimierung des Menschen". Der Bericht äußert Sorgen über die Folgen der Robotik für Bildung, Arbeitswelt und Umwelt und fordert Folgenabschätzungen. Er schlägt Maßnahmen vor, um intelligente Roboter einzustufen und zu registrieren, und eine Pflichtversicherung, um Probleme in Bezug auf Haftungsfragen zu lösen. Zu Interoperabilität, zum Zugang zu Programmiercode und geistigen Eigentumsrechten werden ebenso Empfehlungen ausgesprochen wie zu einer Charta zur Robotik samt Verhaltenskodex für Ingenieure.

Bereits jetzt sind EU-Gesetzestexte vorhanden, die sich mit der Regulierung von Robotern oder Algorithmen beschäftigen. Die neue Datenschutz-Grundverordnung widmet sich der Frage, unter welchen Umständen Mechanismen zur automatisierten Entscheidungsfindung von personenbezogenen Daten möglich sind (Art. 13.2 (f), Art. 14.2(g) und Art. 22). Der Europäische Datenschutzbeauftragte hat einen Ethikrat einberufen, der ihn dabei beraten soll, welche ethischen Folgen eine von Big Data und künstlicher Intelligenz gesteuerte Gesellschaft haben kann. Diese Gruppe ist interdisziplinär und vereint Vertreter verschiedener Stakeholder-Gruppen.

Auch die Richtlinie zu Märkten für Finanzinstrumente (2014/65/EU) fokussiert sich auf Anforderungen der Transparenz, der Sicherheit sowie von Erlaubnispflichten und Risikokontrollen bei Hochfrequenzhandel oder bei algorithmischem Handeln; ebenso die „Delegierte Verordnung", durch die die Richtlinie 2014/65/EU um technische Regulierungsstandards zur Festlegung organisatorischer Anforderungen an Wertpapierfirmen ergänzt werden soll. Auch die Maßnahmen der EU-Kommission zum Internet der Dinge betreffen Algorithmen (siehe dazu der Beitrag von Jürgen Geuter in diesem Band).

Die Robotik wird von der EU bereits reguliert: Die Maschinenrichtlinie widmet sich unter anderem „unvollständigen Maschinen". Dabei handelt es sich um Teilmaschinen, die universell einsetzbar sind und hauptsächlich in der Industrie verwendet werden (wie beispielsweise Schneid-, Lackier-, Sortierroboter in der Automobil- oder Pharmaindustrie). Einige zunächst rein technisch anmutende Kriterien, die in der Richtlinie enthalten sind,

haben eine politische Dimension: So dürfen die Kriterien der Ergonomik nicht auf Größenparametern basieren, die nur der Norm eines männlichen Körpers entsprechen, da dies Frauen unmittelbar diskriminieren oder gar gefährden könnte.

Die EU-Kommission hat zudem Geld in die Erforschung möglicher Regulierung von Robotern investiert, etwa das Projekt RoboLaw, das die gesellschaftlichen Herausforderungen der verschiedenen Anwendungen der Robotertechnologien und deren zukünftige juristische Regulierung betrifft. Auch für die Erforschung und Entwicklung von Robotern haben EU-Kommission und Mitgliedsstaaten Milliardensummen ausgegeben. Die Anwendungsgebiete reichen von Grenzkontrollen (Drohnen, Unterwasserroboter, Bojen, Landroboter) über Medizin und Pflege bis zu Verkehr und Katastrophenhilfe.

Internationale Ebene

In Bezug auf gesetzliche Regulierungen sind die USA weltweit eines der wenigen Länder, die spezifische Robotergesetze entwickelt haben, im Fall der USA für Drohnen und autonome Autos.

Zugleich sind einige Initiativen, Firmenkonsortien und -allianzen sowie private Institutionen entstanden, die sich – in erster Linie unter der Überschrift „künstliche Intelligenz" – der Selbstregulierung widmen. Diese Initiativen beanspruchen zwar meist eine internationale Ausrichtung, befinden sich aber hauptsächlich in der westlichen Hemisphäre. Um einige der prominentesten zu nennen: AI Now, eine interdisziplinäre Forschungsinitiative in New York, bringt namhafte Forscher aus Wirtschaft und Wissenschaft zusammen. Amazon, Facebook, Google, Microsoft und IBM haben 2016 Jahr die Partnership on AI gegründet, um Best Practices zum Einsatz künstlicher Intelligenz zu entwickeln und Öffentlichkeitsarbeit zu machen. Seit Anfang 2017 ist auch Apple Mitglied. Um einiges älter ist die International Federation of Robotics, der internationale Verband der Robotik-Industrie und Robotik-Forschungsinstitute sowie internationaler Dachverband aller nationaler Robotik-Verbände. Der Verband veröffentlicht die Statistik World Robotics über die Roboterinstallationen, Anwenderbranchen, Einsatzzwecke und Robotertypen in etwa 50 Ländern. Darüber hinaus veranstaltet er das traditionelle International Symposium on Robotics (ISR).

In Bezug auf gesetzliche Regulierungen sind die USA weltweit eines der wenigen Länder, die spezifische Robotergesetze entwickelt haben, im Fall der USA für Drohnen und autonome Autos.

Die Praxis der Gründung von Konsortien und Allianzen von Wirtschaftsakteuren, um Best Practices oder Verhaltenskodizes und andere standardisierungsähnliche Mechanismen zu etablieren, ist ebenfalls im Themenfeld Internet der Dinge üblich (vgl. hierzu den Beitrag von Jürgen Geuter), sodass sich die Felder hier überschneiden, denn einige der internetfähigen Dinge (Things) sind komplexe algorithmische Systeme.

Eine weitere relevante Initiative ist Open AI, ein Non-Profit-Forschungsunternehmen für die Entwicklung menschenfreundlicher künstlicher Intelligenz, das vom Tesla-Gründer Elon Musk mit initiiert wurde. Open AI strebt Kooperationen mit anderen Institutionen und Forschern auf freiwilliger Basis an, indem Patente und Forschungsergebnisse öffentlich bereitgestellt werden. Daneben gibt es den Ethics and Governance of Artificial Intelligence Fund, eine Non-Profit-Organisation, die sich zum Ziel gesetzt hat, interdisziplinäre, teilweise normative Forschung und Debatten zur politischen und sozialen Dimension von künstlicher Intelligenz zu führen. Verwaltet wird der Fund vom MIT Media Lab, dem Berkman Klein Center an der Harvard-Universität und den Hauptspendern: eBay-Gründer Pierre Omidyar, Linkedin-Gründer Reid Hoffman und der Knight Foundation. In Deutschland gibt es seit vergangenem Jahr die Advocacy-Organisation AlgorithmWatch, die sich zum Ziel gesetzt hat, über gesellschaftliche Auswirkungen automatisierter Entscheidungsfindung aufzuklären und Regulierungsvorschläge zu entwickeln (Offenlegung: Autorin und Autor dieses Textes sind Mitgründer von AlgorithmWatch).

Open AI strebt Kooperationen mit anderen Institutionen und Forschern auf freiwilliger Basis an, indem Patente und Forschungsergebnisse öffentlich bereitgestellt werden.

Auch internationale, nach dem Multistakeholder-Prinzip arbeitende Standardisierungsorganisationen wie das Institute of Electrical and Electronics Engineers (IEEE) haben eigene Initiativen entwickelt (wie die Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems) und im Dezember 2016 die Studie „Ethically Aligned Design" veröffentlicht. Das IEEE arbeitet an einem Standard mit dem Namen „P7000". Er soll im Entwicklungsprozess künstlicher Intelligenz Systemen helfen, ethische Faktoren explizit zu integrieren. Der US Public Policy Council der Association for Computing Machinery, einer weltweiten Organisation von Praktikern, Lehrenden und Forschern der Informatik, hat Anfang 2017 eine Stellungnahme und sieben Prinzipien zur Transparenz und Überprüfbarkeit von Algorithmen veröffentlicht.

Mit der ISO 13482 hat die Internationale Organisation für Normung (International Organization for Standardization, ISO) 2013 einen Standard für Haushalts- und Assistenzroboter verabschiedet. Vorarbeiten für die Entwicklung eines Standards bei Medizinrobotern haben begonnen, weitere Arbeiten sind noch notwendig. Die ISO fokussiert sich weiterhin auf die reine Sicherheitsnormierung für Roboter. Autonome Entscheidungen spielen dabei keine große Rolle in Sicherheitsstandards, da nach ISO nach dem derzeitigen Stand der Technik kein hoher Grad an Autonomie möglich sei. Die sensorischen Fähigkeiten beschränken sich nur auf vorgegebene Aufgaben. Es gibt kaum Verständnis für die Umgebung und keine Erfassung von Situationen und menschlichen Absichten.

Auch internationale Konferenzen erleben eine Politisierung. Der bekannte RoboCup-Wettbewerb, der ursprünglich als Wettbewerb für Roboterfußball gegründet wurde, avanciert mehr und mehr zu einem Kongress über Roboter mit einem gesellschaftlichen Mehrwert. So läuft parallel zum Fußballwettbewerb ein Kongress über die neuesten wissenschaftlichen Erkenntnisse zu künstlicher Intelligenz und Robotik. Auch in den Wettbewerbssparten gibt es neue Kategorien, die diese Weiterentwicklung reflektieren: neben Rescue-Wettbewerben gibt es auch Home- und Logistik-Wettbewerbe.

Wie einflussreich solche Initiativen und Foren sind, insbesondere mit Blick auf die oben genannten Konsortien und Allianzen, kann am Beispiel des Future of Life Institute verdeutlicht werden. Mit berühmten Förderern und Unterstützern wie Stephen Hawking und Elon Musk fokussiert sich das Institut auf die Entwicklung von ethischer künstlicher Intelligenz und ist führend in der politischen Debatte zur künstlichen Intelligenz und Politik. Musk und das Institut organisierten die Open Letter on Autonomous Weapons mit namhaften Unterzeichnern. Davor hatte der UN Rapporteur for Extrajudicial Executions für internationale Regeln in Bezug auf bewaffnete Roboter plädiert.

Ein Jahr nach Unterzeichnung des Briefes haben 89 Länder im Verlauf der UN International Convention on Conventional Weapons in Genf entschieden, mit Expertengruppen 2017 ein mögliches Verbot von autonomen Waffen und autonomen bewaffneten Robotern zu prüfen ("UN has decided to tackle the issue of killer robots in 2017"). ■

Getränkeautomat legt Uni lahm

Das Internet der Dinge stellt nationale wie internationale Organisationen vor große Herausforderungen. Verbraucherschutz, Haftungsrecht und Sicherheit sind nur einige der Themen.

JÜRGEN GEUTER

Von intelligenten Stromzählern über sich an persönliche Vorlieben anpassende Heizungssteuerungen bis hin zu Netzwerken aus Sensoren und zu Fabrikationsanlagen, die sich zu Smart Factories zusammenschalten: Internetverbundene Geräte haben Einzug in den Alltag gehalten, privat wie beruflich. Die Regulierung dieser neuartigen Datensammler und -auswerter stellt nationale wie internationale Organisationen vor große Herausforderungen. Ein konsistentes Vorgehen wird erschwert durch die global sehr heterogenen Regulierungsansätze sowie durch die Vielfalt der Themen und Politikfelder, die von dem Internet of Things (IoT) tangiert werden. Dazu zählen vor allem Belange des Daten- und Verbraucherschutzes, des Wettbewerbsrechts, der Strafverfolgung, des Sachenrechts, des Haftungs- und Medizinrechts sowie der technischen Sicherheit.

Kurzum: Der Einsatz von internetfähigen Geräten betrifft im Prinzip alle Lebensbereiche und Berufssparten, in denen sie eingesetzt werden, und somit die entsprechenden Rechtsgebiete. Gesetzgeberische Entscheidungen und technische Regeln haben in diesen Bereichen oftmals deutliche gesellschaftspolitische Auswirkungen. International setzten insbesondere die durch US-Unternehmen definierten technischen Regeln einen regulativen Quasi-Standard. Nationale Gesetzgebung hat es oft schwer, sich dagegen zu behaupten. Insbesondere auf nationaler Ebene wird zudem ein transparenter öffentlicher Meinungsbildungsprozess dadurch erschwert, dass die im Bereich des Querschnittsthemas IoT engagierten Akteure mit sehr unterschiedlichen Ressourcen ausgestattet sind.

Das Internet der Dinge

Die Idee des „Intelligenten Kühlschranks" konnte man schon Ende der 1990er-Jahre in Berichten zur alljährlichen CeBIT finden. Durch Verbindung zum noch jungen Internet sollten gewöhnliche Haushaltsgeräte den Alltag vereinfachen, zum Beispiel indem sie – im Falle des viel zitierten Kühlschranks – rechtzeitig vor Ausgehen der Vorräte online Milch, Eier und Käse nachbestellen. In den letzten Jahren wurde dieser Ansatz, herkömmliche Haushaltsgeräte durch Anbindung ans Internet „smart" zu machen, von etablierten Marken wie von neuen Start-ups vermehrt aufgegriffen. Auch „Smart Meter", d.h. intelligente Stromzähler, haben starke Verbreitung gefunden. Smart Meter empfangen Daten etwa über Stromtarife, während sie gleichzeitig Daten zum Stromverbrauch des Abnehmers an den Erzeuger weitergeben. Energieversorgungsunternehmen und Endkunden wird so eine effizientere Planung von Energiebereitstellung und -verbrauch ermöglicht.

In den letzten Jahren wurde der Ansatz, herkömmliche Haushaltsgeräte durch Anbindung ans Internet „smart" zu machen, von etablierten Marken wie von neuen Start-ups vermehrt aufgegriffen.

In einer zweiten Phase kam eine neue Generation kleinerer und günstigerer Geräte mit Online-Anschluss auf den Markt. Neuere IoT-Anwendungen zeichnen sich – im Unterschied zu den ersten Zukunftsvisionen Ende der 1990er-Jahre – dadurch aus, dass sie selbst allein kaum ‚Intelligenz' mitbringen. Vielmehr beziehen diese Geräte ihre ‚Intelligenz' ausschließlich durch zentrale, cloudbasierte Dienste. Ein Beispiel: tragbare Sensoren („Wearables"), erlauben es, zu Fuß zurückgelegte Strecken oder den eigenen Puls über den Tagesverlauf hinweg aufzuzeichnen und diese Informationen an Online-Dienste weiterzuleiten. Die aufgenommenen Werte können dann automatisiert analysiert werden und die Basis für individuelle Verhaltensvorschläge liefern: Die Uhr am Handgelenk erinnert ihren Träger oder ihre Trägerin daran, eine Pause zu machen und ein paar Schritte zu laufen. Komplexere Ratschläge auf Basis des permanent

mitgeschriebenen Blutdrucks und dem gleichzeitig erfassten Ort können in Warnungen münden wie: „Du hast schon den ganzen Tag gesessen und solltest jetzt wirklich kein Fast Food essen."

Nicht nur im Privatbereich spielt das Internet der Dinge eine zunehmende Rolle. Auch die Industrie entwickelt unter den Überschriften „Industrie 4.0" und „Smart Factories" IoT-Konzepte: Alte Anlagen sollen beispielsweise mit günstigen Sensoren in die moderne digitale Fabrik eingebettet werden. Kleine, günstige Sensoren innovativer Hersteller liefern als Ad-hoc-Informationsquelle im Fabriknetzwerk Informationen zur Prozesssteuerung. „Virtuelle Fabriken", das heißt sich aus einem Pool an Anlagen immer wieder neu und anders zusammenschaltende Produktionslinien, erlauben es Unternehmen, sich innerhalb von kürzesten Zeiten neu zu konfigurieren, um auf neue, kurzfristige Kundenwünsche zu reagieren. Im Extremfall wäre denkbar, dass erst nach dem Auftrag eines Kunden eine Produktionsstraße definiert wird, die alle notwendigen Maschineneinstellungen automatisch vornimmt und diese über dezentrale Umgebungssensoren in Echtzeit anpasst. Den Transport der Zwischenprodukte übernehmen intelligente autonome Förderfahrzeuge und Roboter, die die Artikel per RFID oder ähnlicher Technologie erkennen und sie automatisch zum nächsten Prozessschritt fahren.

Unter dem Schlagwort der „Smart City" werden diverse Versuche und Ansätze zusammengefasst, die öffentliche Infrastruktur durch Sensorik und Netzanbindung in ein digitales Abbild der Stadt zu verwandeln.

Das Internet der Dinge ist auch im nicht kommerziellen Kontext ein großes Thema. Unter dem Schlagwort der „Smart City" werden diverse Versuche und Ansätze zusammengefasst, die öffentliche Infrastruktur durch Sensorik und Netzanbindung in ein digitales Abbild der Stadt zu verwandeln. Durch diese ‚virtuelle Stadt' kann automatisiert auf Gegebenheiten wie Verkehrsstau oder die Überschreitung von Abgasgrenzwerten reagiert werden, um die Abläufe in der Stadt effizienter zu gestalten oder Ressourcen zu schonen.

Das Internet of Things, das heisst die Anbindung von relevanten Anlagen oder Geräten ans Internet, zieht sich also schon heute durch nahezu alle Lebensbereiche. Nationale wie internationale Regulierung stehen vor einer neuen Herausforderung, die sehr unterschiedlichen Interessen, Rechte und Rechtsnormen aller Stakeholder miteinander in Einklang zu bringen.

Juristische und ‚pragmatische' Regulierung

Regulierung im engeren Sinne meint den staatlichen oder staatsähnlichen regulativen Eingriff: Die Schaffung von Gesetzen, EU-Verordnungen und Richtlinien. Hinzu kommen technische Regeln, das heißt (konsensuell

erstellte) Normen sowie Standards (im Sinne anerkannter und vereinheitlichter Praktiken der Herstellung oder der Durchführung). Normen und Standards sind das Resultat des organisierten Handelns von Firmen und anderen technischen Organisationen, wie beispielsweise des Institute of Electrical and Electronics Engineers (IEEE), der Internet Engineering Task Force (IETF) oder der International Organization for Standardization (ISO), die die Hardware- und Softwareplattformen des IoT definieren, entwickeln und vorantreiben.

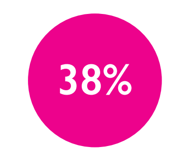
Stoßrichtungen der IoT-Regulierung

Weil das „Internet of Things" ein breiter Sammelbegriff ist, unter dem Objekte sehr unterschiedlicher sozialer Einbettung wie auch technischer Komplexität und Leistungsfähigkeit subsumiert werden, treffen bei seiner Regulierung eine Vielzahl bestehender Regulierungen und Regulierungstraditionen aufeinander.

IoT-Geräte – insbesondere jene für den Privatgebrauch – werden oft personalisiert beziehungsweise im persönlichen Wohnraum platziert, um dort Daten zu erheben und mit Menschen zu interagieren. Bestehende Datenschutzgesetzgebung bzw. deren Adaption oder Neukalibrierung auf neue Anwendungskontexte treibt deshalb einen sehr großen Teil aktueller Regulierungsbestrebungen bezüglich des IoT voran. Dabei können selbst scheinbar eher harmlose Einsatzzwecke (wie zum Beispiel die automatische Anpassung der Raumtemperatur an die bevorzugte Temperatur der im Raum befindlichen Personen) datenschutzrechtlich Konsequenzen mit sich bringen, da ein Thermometer implizit Bewegungsprofile der Personen in der Wohnung erzeugen kann. Im privaten Kontext sind auch Aspekte des Verbraucherschutzes zu adressieren: Ein Fehler in der Heizungssteuerung kann nicht nur zu einer unangenehmen Raumtemperatur führen, sondern auch zu einem deutlich erhöhten Energieverbrauch und damit erhöhten Kosten. Sogar gesundheitliche Konsequenzen sind nicht auszuschließen, wenn softwaregesteuerte, mit dem Internet verbundene Geräte im privaten Wohnraum Einzug halten: Für Menschen mit Epilepsie beispielsweise könnte ein Fehler (oder eine Sicherheitslücke) in internetverbundenen Lichtsteuerungen im Extremfall zu einem epileptischen Anfall führen.

Die neuen Plattformen für IoT-Geräte werfen immer wieder Fragen des Wettbewerbsrechts auf. Die größeren Geräte- und Softwarehersteller genießen bereits eine gewisse Marktmacht und haben somit aufgrund ihrer Ressourcen einen Wissens- und Wettbewerbsvorteil in spezifischen Bereichen (im Privaten, durch Assistenzgeräte im Haushalt wie im

Die wichtigsten Regulierungsfragen für das Internet der Dinge



steigende Sicherheitsrisiken



Privatsphäre



Identitäts- und Zugangsverwaltung



Angriffe auf IoT-Geräte



Regelbefolgung (Compliance)



Daten außerhalb eigener Firmen-IT

5%



Anfragen zur Datenherausgabe, z.B. von Ermittlungsbehörden

2%



andere

2%

keine

Quelle: ISACA: Internet of Things. Risks and Value Consideration 2013

Professionellen, durch Assistenzsysteme im Betrieb). Statt neuen Unternehmen und Projekten Zugang zum Markt zu ermöglichen, könnten die neuen digitalen Plattformen zu neuen Monopolen führen.

Schließlich kommen noch die technische Sicherheitsstandards zum Tragen. Die Funkfrequenzen, auf denen viele der IoT-Anwendungen Daten austauschen, werden – wie beispielsweise bei WLAN oder Bluetooth – durch internationale Standards definiert und weltweit etabliert. Sie können aber regional leicht unterschiedliche Ausprägungen haben. Auch für den Einsatz bestimmter, standardisierter Technologien und Protokolle in unterschiedlichen Domänen (Industrie, öffentliche Infrastruktur, Gesundheitswesen) sind die technischen Sicherheitsstandards in permanenter Weiterentwicklung begriffen, um neuen Risikopotenzialen oder neuen sozialen Praktiken zu begegnen.

Seiner Verbreitung und tiefen Integration wegen ist die Frage der IT-Sicherheit im Kontext des IoT noch gesondert zu erwähnen. Ein kleiner Fehler im Code eines scheinbar unscheinbaren IoT-Devices kann durch die schlichte Menge der Geräte gravierende Konsequenzen haben. Selbst große Webseiten können etwa durch einen plötzlichen Angriff von Millionen von „smarten" Glühbirnen zu Fall gebracht werden („Zig Bee-Wurm befällt smarte Glühbirnen"). Getränkeautomaten haben schon mal das Internet einer Universität lahmgelegt („Universität von eigenem Getränkeautomaten angegriffen"). Ein solches Szenario im Kontext von Verkehrssteuerung oder in potenziell gefährlichen Industrieprozessen ist in seinen Konsequenzen kaum noch abschätzbar. Anforderungen an Sicherheit stehen in einem deutlichen Spannungsverhältnis zu den Marktmechanismen. Neue IoT-Produkte – insbesondere im Endverbraucherbereich – haben kurze Entwicklungszyklen und oft eher geringe Margen. Technische Sicherheit ist hier nicht immer ausreichend gewährleistet.

Die technischen Sicherheitsstandards sind in permanenter Weiterentwicklung begriffen, um neuen Risikopotenzialen oder neuen sozialen Praktiken zu begegnen.

Diese sehr unterschiedlichen, teils widersprüchlichen Regulierungsziele (Wettbewerb und Innovation sowie Sicherheit) miteinander zu harmonisieren ist schon auf der nationalen Ebene alles andere als einfach. Im internationalen Kontext wird diese Aufgabe jedoch noch um ein Vielfaches komplexer.

Internationale Regulierung des IoT

Auf globaler Ebene spielen die Vereinten Nationen (UN) selbstverständlich eine gewichtige Rolle. Als dominanter globaler politischer und diplomatischer Diskursraum im Bereich der Grundrechte haben die UN einen

großen Einfluss auf die im Bereich der IoT-Regulierung laufenden internationalen Debatten, die immer auch Menschenrechtsthemen berühren. So riefen die UN im Jahr 2006 das Internet Governance Forum (IGF) ins Leben, welches als Multistakeholder-Forum eine Plattform zu Themen um das Internet bietet. Aufgabe des IGF ist es nicht nur, laufende Debatten zu begleiten und zu strukturieren, sondern auch, aufkommende Herausforderungen, Probleme oder Risiken frühzeitig zu erkennen und zu analysieren. Im Rahmen des IGF ist eine internationale Arbeitsgruppe entstanden, die Dynamic Coalition on the Internet of Things, welche Good Practices herausarbeitet. Das IGF hat dabei allerdings keinerlei politische Entscheidungsbefugnis oder Legitimation.

Aufgabe des IGF ist es nicht nur, laufende Debatten zu begleiten und zu strukturieren, sondern auch, aufkommende Herausforderungen, Probleme oder Risiken frühzeitig zu erkennen und zu analysieren.

Etwas näher an entscheidungsbefugten Strukturen der UN befinden sich die diversen United Nations Special Rapporteurs, welche als Individuen von der UN beauftragt werden, sich mit spezifischen Aspekten oder Bedrohungen für die globale Durchsetzung der Menschenrechte zu befassen. Die Rapporteurs sind zwar selbst ebenso wie das IGF nicht entscheidungsbefugt, haben jedoch Berichtsmöglichkeiten gegenüber einer breiten Öffentlichkeit und genießen hohe Autorität im Kreise der Vereinten Nationen. Die Rapporteure ergänzen die eher horizontalen Betrachtungen des IGF durch vertikale, auf spezifische Themenkomplexe ausgerichtete Detailanalysen wie zum Beispiel zu „Privacy“, „Education“, „Freedom of Expression“ oder „Health“. Dies alles sind Politikfelder, die vom Internet der Dinge tangiert sind.

Mit der Sicherstellung eines möglichst freien Informationsflusses als einem ihrer Kernziele findet sich auch die UNESCO als Teil der UN immer wieder im Zentrum der internationalen Debatten um die Regulierung des Internets – und somit auch des IoT. Im Bereich der Regulierung wirkt die UNESCO ebenfalls vor allem beratend als publizierende Institution.

Neben der UN spielen auch europäische Organisationen und Gremien eine relevante Rolle im Kontext der Regulierung des IoT. So schaltet sich beispielsweise der Datenschutzbeauftragte der EU aktiv in internationale Debatten ein.

All diese unterschiedlichen Foren, Organisationen und Individuen gestalten die internationalen Debatten um die Regulierung des Internets, nehmen Spezialisten-Input auf und sorgen aktiv für einen internationalen Austausch zur Etablierung gemeinsamer Werte, die sich im besten Fall in konkreter Gesetzgebung niederschlägt.

Im Bereich der Standardisierung der IoT-Technologien werden wichtige Regeln immer noch hauptsächlich von Firmen definiert. Als besonders sichtbare Firmen geben Google und Apple mit ihren Plattformen „Weave“ und „Homekit“ technische Standards vor. Dies geschieht auch über die Gründung von Allianzen und Konsortien mit anderen Unternehmen oder Verbänden. Die Maßnahmen zielen auf eine Beschleunigung in der Standardisierungsentwicklung in Bezug auf bestimmte Produktkategorien oder Märkte, um sicherzustellen, dass die Technologien ihrer Mitglieder in anerkannten Standards verankert werden. Beispiele hierfür sind Bluetooth Special Interest Group, ZigBee Alliance, Wi-Fi Alliance, die Organization for the Advancement of Structured Information Standards (OASIS), and the Silicon Integration Initiative (Si2), die sich Electronic Design Automation widmet (EDA), sowie die Open Mobile Alliance (OMA), die Spezifikationen für Interoperabilität für End-to-end Mobile Services entwickelt. Ein weiterer Akteur ist die MIPI Alliance, eine internationale Organization, die Spezifikationen für die Benutzeroberflächen für industrieorientierte Mobile-Anwendungen entwickelt. Keine dieser Gruppen ist eine Standardisierungsorganisation im engeren Sinne, jedoch sind viele ihrer Mitglieder aktive Teilnehmer in den Prozessen von Standardisierungsgremien, beispielsweise hinsichtlich der Industriestandards der IEEE (IEE IoT Related Standards). Letztere sind oft eher darauf ausgerichtet, die Interoperabilität und Kompatibilität der bestehenden Industrieprotokolle und Technologien voranzutreiben. ISO fokussiert sich unter anderem auf Sicherheitsstandards. CEN, das Europäische Komittee für Standardisierung der EU, hat seinen Standardisierungsschwerpunkt auch in der Frage der Interoperabilität, des Umwelt- und Verbraucherschutzes sowie der Sicherheit. Die WTO will mit seiner Technical Barriers to Trade Agreement (TBT) möglichst effiziente Standards und Handelshemmnisse abbauen. Darin werden im Code of Conduct die Vorteile und die Notwendigkeit von internationaler Standards festgestellt, wenn auch der Bedarf für landes- und regionalspezifische Standards anerkannt wird. So unterzeichneten CEN und ISO die Wiener Vereinbarung (1991), um eine Duplikation von Standards zu vermeiden und ihre Kooperation effizienter zu gestalten. Die meisten der oben erwähnten technischen Institutionen sind offen: Jeder, der will, darf sich beteiligen und Vorschläge senden. Die Anzahl der dort beteiligten Wirtschaftsakteure ist recht hoch, doch auch Regierungsspezialisten und Zivilgesellschaft (mit NGOs wie bspw. Article 19 oder Verbraucherschutzverbände) nehmen daran teil.

Im Bereich der Standardisierung der IoT-Technologien werden wichtige Regeln immer noch hauptsächlich von Firmen definiert.

Im Kontext des IoT spielt hier – neben den bestehenden rechtlichen Debatten in Sachen- und Haftungsrecht – die Verabschiedung der EU-Datenschutz-Grundverordnung (DGVo) sicherlich die größte Rolle. Die DGVo

stellt für die Erfassung und auch die Weiterverarbeitung personenbezogener Daten hohe Hürden auf und definiert insbesondere die Anforderungen an die Einwilligung von Datenerhebung und -verarbeitung Betroffener. Persönliche IoT-Devices – wie Herzfrequenztracker – sind hiervon weniger tangiert als die an Popularität gewinnenden Sprachassistenten wie Google Home oder Amazons Alexa. Jeder und jede Besuchende einer Wohnung, in der ein Sprachassistent eingesetzt wird, müsste eigentlich explizit in die Datenaufzeichnungen einwilligen. SmartTVs, die ähnliche Funktionen eingebaut haben, stehen vor demselben Problem. Hier steht internationale EU-Regulierung direkt und massiv den strategischen Interessen global agierender Unternehmen wie Amazon, Google und Sony gegenüber, die nun auf die einzelnen Staaten innerhalb der EU (und die EU selbst) einwirken, um Ausnahmen oder Workarounds für diese Form der Datenerhebung zu etablieren. Die EU-Kommission gründete im März 2015 die Alliance for Internet of Things Innovation (AIOTI), eine offene Plattform für die Entwicklung von Forschung und Best Practices. Auch die Strategien der EU-Kommission zum digitalen Binnenmarkt sowie „Digitizing European Industry“ setzen das IoT als zentrales Thema. Die Kommission kündigte an, im Rahmen dieser Strategien gemeinsam mit allen Stakeholdern zum IoT arbeiten zu wollen. Auch Bereiche der DG Connect „Data Economy“ erfassen das Internet der Dinge.

Die EU versucht die Etablierung von IoT-Standards durch Forschungsförderung auch im Rahmen des aktuellen Framework-Programms FP7 zu begleiten und zu formen. Der Fokus liegt hier darauf, die direkten Interessen des öffentlichen Sektors im Bereich der Smart Cities voranzutreiben – mit Projekten wie ALMANAC (www.almanac-project.eu), SMARTIE (smartie-project.eu) oder CLOUT (clout-project.eu). Die Projekte beschäftigen sich alle mehr oder weniger damit, Smart Cities mit den bestehenden Europäischen Regulierungen zu vereinbaren, insbesondere mit Blick auf Datenschutz und Sicherheit.

Die EU versucht die Etablierung von IoT-Standards durch Forschungsförderung auch im Rahmen des aktuellen Framework-Programms FP7 zu begleiten und zu formen.

Regulierung in den USA

Auch wenn die Regulierung des IoT innerhalb der USA eigentlich als nationale Regulierung zu betrachten ist, so hat sie doch im Kontext des Internets international Tragweite. Als Großmacht und Sitz einiger der wichtigsten Technologiecluster und als einer der größten Märkte für IoT-verwandte Produkte geben die USA mit ihrer nationalen Regulierung faktisch den Takt für den internationalen Einsatz und damit auch die Regulierung von IoT-Devices vor. Ein prominenter Fall: 2014 ging die US Federal Trade Commission (FTC) erfolgreich gegen die Firma Vizio vor, die mit ihrer Software

auf SmartTVs seit 2014 die detaillierten Sehgewohnheiten der Nutzenden ohne deren Einwilligung mitschrieb („VIZIO to pay 2.2 million to FTC"). Der Auseinandersetzung VIZIO v. FTC kann dabei durchaus Mustercharakter zugesprochen werden. Sehr ähnlich gelagerte Fälle betreffen den gesamten Bereich der Sprachassistenten. Zur Aufklärung von Verbrechen insbesondere im privaten Kontext hat die Polizei ein großes Interesse, auf die durch die Sprachassistenten aufgezeichneten Daten zuzugreifen („Can Alexa help to solve a murder?"). Die zu diesem Thema in den USA etablierten Vorgaben haben Referenzcharakter für Entwicklungen in Europa oder anderswo auf der Welt.

Somit kommt der US-Regierung und Behörden wie der FTC ein fast globaler Einfluss zu. Andere rechtliche Räume müssen entweder zum rechtlichen Rahmen der USA kompatibel sein oder einen sehr umsatzstarken Markt darstellen, um den Aufwand einer regionalen Anpassung zu rechtfertigen.

Regulierung des IoT in Deutschland

Im Bereich des Internet of Things befindet sich Deutschland weitgehend in einer Konsumentenposition: Die Technologie und ihre Artefakte werden oft weder in Deutschland noch explizit für den deutschen Markt gefertigt. Das stellt die Regulierung vor besondere Herausforderungen. So können deutsche Regulierer oft erst am fertigen Produkt ansetzen und nicht schon den Entstehungsprozess begleiten. Produkte, die seit Monaten wenn nicht gar Jahren in den USA eingesetzt werden, gehen einher mit sozialen Praktiken, die die Menschen in Deutschland über die Darstellung in US-Medien mit dem Produkt verbinden – egal ob die Praktiken mit deutschem oder europäischem Recht konsistent sind.

In Deutschland sind vor allem das Justizministerium (welches auch für Verbraucherschutz zuständig ist) und das Innenministerium als zuständige Behörden zu nennen, welche gemeinsam einen großen Teil der schon angesprochenen Regulierungsdomänen abdecken. Hinzu kommen auch immer wieder Initiativen des Ministeriums für Bildung und Forschung, das laufende Forschungsschwerpunkte in die Debatte einbringt.

Auch der oder die Beauftragte für Datenschutz und Informationsfreiheit berät und begleitet Gesetzes- und Regulierungsvorhaben im Kontext des Internets der Dinge

Auch der oder die Beauftragte für Datenschutz und Informationsfreiheit berät und begleitet Gesetzes- und Regulierungsvorhaben im Kontext des Internets der Dinge, kann aber auch durchaus proaktiv tätig werden und durch Gutachten und Vorschläge auf die öffentliche Meinungsbildung und den folgenden gesetzgebenden Prozess einwirken.

Diverse mehr oder weniger einflussreiche politische NGOs und Interessenverbände nehmen immer wieder als Experten oder Gutachtende an den Diskussionen um neue Regeln oder eine Adaption bestehender Regeln teil. Insbesondere im Bereich der aufs Digitale ausgerichteten NGOs hat sich auch eine sehr konkrete Arbeit an Gesetzestexten beziehungsweise der Zulieferung von konkreten Formulierungsvorschlägen in Richtung der Legislative etabliert.

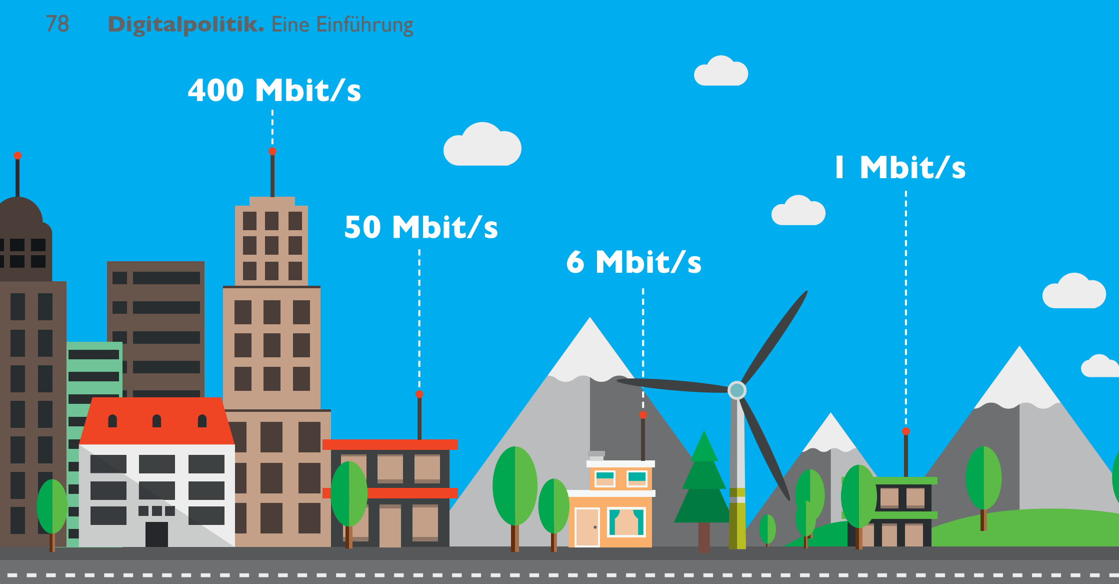
Zusammenfassung

Neben den sich in hohem Tempo verändernden technologischen Rahmenbedingungen ist die Pluralität der auf das Themenfeld „Internet of Things" einwirkenden Akteure eine große Herausforderung für Politik und Gesellschaft. Die notwendige Transparenz in Entscheidungen, die von öffentlichem Interesse sind, ist dadurch nicht immer gewährleistet.

Die gesetzliche Regulierung des Internets der Dinge in den USA setzt gemeinsam mit den insbesondere durch US-Unternehmen definierten technischen Regeln den regulativen Quasi-Standard.

Internationale Organisationen (meist aus dem UN-Umfeld) versuchen, den Debatten vor allem durch Berichte und strukturierte Diskussionen einen gewissen Rahmen zu geben und somit einen globalen Wissensstand herbeizuführen, der unterschiedliche Wünsche und Bedürfnisse widerspiegelt. Die gesetzliche Regulierung des Internets der Dinge in den USA setzt gemeinsam mit den insbesondere durch US-Unternehmen definierten technischen Regeln den regulativen Quasi-Standard. Dies bringt insbesondere kleinere Staaten in eine sehr schwierige Position bei der Durchsetzung nationaler Regeln.

Während international stark auf Multistakeholder-Ansätze gesetzt wird, stellt sich die Situation in Deutschland etwas traditioneller dar: Wenige spezialisierte NGOs und Lobbygruppen von wirtschaftsnahen Organisationen wie BITKOM und Eco bis hin zu bürgerrechtlich orientierten Organisationen wie der Chaos Computer Club oder die Digitale Gesellschaft versuchen – teils im Bündnis, teils im Alleingang –, auf den Meinungsbildungsprozess der Regierung und des Parlaments Einfluss zu nehmen. Hier wäre ein strukturierterer und transparenterer Multistakeholderprozess, wie auf internationaler Ebene etabliert, ein wichtiger Schritt, um ein Querschnittsthema wie das Internet der Dinge nicht anhand kleiner Detailprobleme und -anforderungen zu debattieren, sondern als grundsätzliche Frage, die fast jeden Teil menschlichen Lebens mittel- oder unmittelbar berührt. ■



Anschluss für ländliche Regionen

In Deutschland ein Thema, aber auch international: Breitbandausbau. Für Diskussionen sorgen nicht nur technische Details, sondern auch die monopolartige Position einzelner Anbieter.

HAUKE GIEROW

Die Internetgeschwindigkeiten in vielen Regionen Deutschlands sind nach wie vor gering. Oft nur wenige Kilometer von Metropolen wie Berlin oder München entfernt, können Kunden nur Internetanschlüsse mit einer Leistung von teilweise weniger als 10 Megabits pro Sekunde buchen. Insbesondere für Unternehmen ist das oft nicht genug. Auf eigene Faust einen Glasfaseranschluss legen zu lassen übersteigt jedoch meist Investitionswillen und -fähigkeit der oft mittelständischen Unternehmen. In einigen Kommunen gibt es nach wie vor kein Breitband-Internet über einen Festnetz- oder Kabelanschluss, sondern nur Verträge mit begrenztem Datenvolumen über den Mobilfunkstandard LTE. Politischer Handlungsbedarf besteht hier insofern, als Akteure, die auf dem Markt eine zentrale Stellung einnehmen – vor allem die Deutsche Telekom – zum Teil nur bedingt für

die notwendige Verbesserung in der Versorgung aktiv werden. Strittig sind auch einige technische Details zur Realisierung einer flächendeckenden leistungsfähigen Internetversorgung. Hier geht es unter anderem darum, ob die von der Bundesregierung gesteckten Ziele ausreichend sind, um den Bedürfnissen gerecht zu werden. Ein anderes Thema ist der Umgang mit Technologien, die eine monopolartige Stellung einzelner Anbieter in Regionen befördern und sich insofern nachteilig für Verbraucher auswirken könnten.

International stehen die Überwindung des Digital Divide auf der Agenda sowie die Modalitäten des Ausbaus der Internetversorgung. Umstritten ist hier vor allem das Engagement von Unternehmen und anderen Organisationen, die mit Angeboten wie Facebook Free Basics oder Wikipedia Zero zwar einen kostenlosen, beschränkten Internetzugang ermöglichen, dabei aber möglicherweise das Prinzip der Netzneutralität verletzen und eigene Dienste bevorzugen.

Ausbau bis 2025

Der Ausbau der Breitband-Versorgung ist Gegenstand der Digitalen Agenda der Bundesregierung. Bis zum Jahr 2018 sollen alle Haushalte mit einer Geschwindigkeit von mindestens 50 Megabit pro Sekunde an das Internet angeschlossen werden. Bis 2025 soll ein flächendeckendes Gigabit-Netz entstehen. Für die Breitbandförderung stellt die Bundesregierung in den kommenden Jahren vier Milliarden Euro an Fördergeldern zur Verfügung. Die Bundesländer können sich auf diesen Topf bewerben, müssen aber Eigenleistungen erbringen – die Förderung deckt 50 bis 70 Prozent der „zuwendungsfähigen Kosten“ ab. Die Gesamtkosten für den flächendeckenden Ausbau auf 50 Megabit pro Sekunde wird mit rund 20 Milliarden Euro beziffert. Das von der Bundesregierung geplante Gigabit-Netz soll unter Einbeziehung des derzeit in Entwicklung befindlichen 5G-Standards erfolgen. Ob dieser Standard ein vollwertiger Ersatz für den Glasfaserausbau ist, gilt jedoch als umstritten. Ein kompletter Glasfaserausbau für alle Haushalte in Deutschland würde Berechnungen des TÜV Rheinland und der TU Dresden zufolge rund 93 Milliarden Euro kosten.

Der Ausbau der Breitband-Versorgung ist Gegenstand der Digitalen Agenda der Bundesregierung.

Von Seiten der Regierungspolitik ist das Thema „Digitale Infrastruktur" seit dem Kabinett Merkel III in der Großen Koalition vom Bundesministerium für Wirtschaft und Energie in das Bundesverkehrsministerium gewechselt, das seitdem auch den Namenszusatz „für Digitale Infrastruktur“ trägt und neben dem Bundesministerium für Wirtschaft und Energie sowie dem Justiz- und Verbraucherschutzministerium ebenfalls eine Führungsrolle bei der Um- und Durchsetzung der Digitalen Agenda beansprucht.

Aufseiten der Provider gibt es neben dem ehemaligen Monopolisten, der Deutschen Telekom, mittlerweile zahlreiche kleine und regionale Anbieter, wie etwa Hanse.net, Wilhelm.tel, die Deutsche Glasfaser und EWE, im Koaxialnetz (TV-Kabelnetz) außerdem Vodafone (ehemals Kabel Deutschland) und Unitymedia (vor allem in Süddeutschland aktiv). Über das Kabelnetz lassen sich bereits heute Geschwindigkeiten von bis zu 400 Megabit pro Sekunde erreichen, in Zukunft soll durch den Docsis-3.1-Standard noch deutlich mehr möglich sein. Im Unterschied zum direkten Glasfaseranschluss hat aber nicht jeder Kunde seine eigene Leitung, vielmehr ist das Koaxialnetz ein Shared-Medium, bei gleichzeitiger sehr hoher Ausnutzung kann es daher bei einzelnen Kunden zu Geschwindigkeitseinbußen kommen.

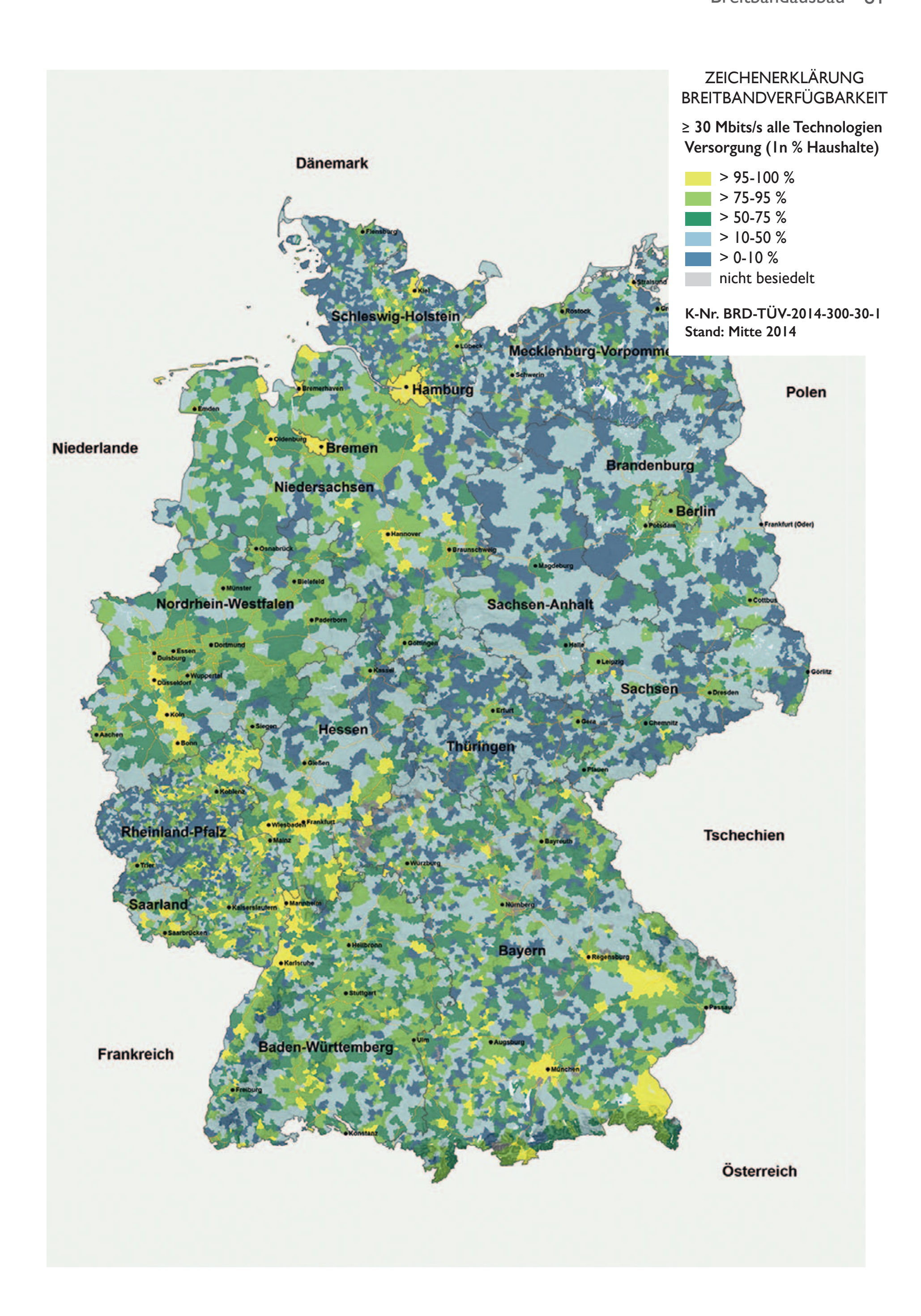
Viele der Telekom-Wettbewerber haben sich im Bundesverband Breitbandkommunikation e.V. (Breko) zusammengeschlossen. Nach eigener Angabe hat der Verband rund 270 Mitglieder, von denen etwa 150 auf regionaler Ebene aktiv sind. Die Kabelnetzbetreiber sind im Verband Anga zusammengeschlossen.

Glasfaser vs. Vectoring und G-Fast

Unter den Providern gibt es unterschiedliche Prioritäten für die technischen Mittel beim Ausbau. Die Deutsche Telekom als größter deutscher Netzbetreiber strebt zurzeit keinen flächendeckenden Glasfaserausbau bis ans Haus (Fibre-to-the-Home FTTH) an, sondern bevorzugt das sogenannte Vectoring. Beim Vectoring wird Glasfaser nur bis zum Verteilerkasten an der Straße ausgebaut. Eine erhöhte Datenrate beim Kunden wird dann erreicht, indem die Spannung auf den bestehenden Glasfaserkabeln erhöht wird. Mit Vectoring sind derzeit unter idealen Bedingungen Datenraten von 50 bis 100 Gigabit im Downstream möglich. Eine symmetrische Anbindung für Up- und Downstream ist nicht vorgesehen.

Da die Glasfaser nicht bis zum Haus, sondern nur bis zur Bordsteinkante ausgebaut wird, spricht man auch von Fibre-to-the-Curb (FttC). Die Telekom bietet Kunden auf Wunsch einen selbst finanzierten Ausbau der Glasfaserinfrastruktur bis ans Haus an (FTTH). Zahlreiche konkret angeforderte Angebote zeigen jedoch, dass das wirtschaftlich für kaum einen Kunden realisierbar ist, da die Kosten zum Teil mit mehr als 50.000 Euro angesetzt werden. Wettbewerber der Telekom bieten einen solchen Ausbau für einen Bruchteil des Preises an.

Das Vectoring ist vor allem unter den Konkurrenten der Telekom umstritten, weil immer nur ein einziger Anbieter die Technologie in einem


ZEICHENERKLÄRUNG
BREITBANDVERFÜGBARKEIT
≥ 30 Mbits/s alle Technologien
Versorgung (In % Haushalte)
> 95-100 %
> 75-95 %
> 50-75 %
> 10-50 %
> 0-10 %
nicht besiedelt
K-Nr. BRD-TÜV-2014-300-30-1
Stand: Mitte 2014
Dänemark
Schleswig-Holstein
Mecklenburg-Vorpomme
Hamburg
Bremen
Niederlande
Niedersachsen
Brandenburg
Berlin
Polen
Nordrhein-Westfalen
Sachsen-Anhalt
Sachsen
Hessen
Thüringen
Rheinland-Pfalz
Saarland
Tschechien
Bayern
Frankreich
Baden-Württemberg
Österreich
Flensburg
Kiel
Rostock
Lübeck
Schwerin
Bremerhaven
Emden
Oldenburg
Potsdam
Frankfurt (Oder)
Hannover
Osnabrück
Braunschweig
Magdeburg
Münster
Bielefeld
Cottbus
Paderborn
Essen
Dortmund
Duisburg
Göttingen
Halle
Wuppertal
Düsseldorf
Kassel
Leipzig
Görlitz
Dresden
Köln
Erfurt
Gera
Chemnitz
Aachen
Siegen
Bonn
Gießen
Plauen
Koblenz
Wiesbaden
Frankfurt
Mainz
Bayreuth
Trier
Würzburg
Kaiserslautern
Mannheim
Nürnberg
Saarbrücken
Heilbronn
Regensburg
Karlsruhe
Stuttgart
Passau
Ulm
Augsburg
München
Freiburg
Konstanz

bestimmten Ortsnetz anbieten kann. Aus diesem Grund wurde sogar die EU-Kommission eingeschaltet, um das exklusive Vectoring durch die Telekom in vielen Gemeinden zu ermöglichen. Die Kommission hat die Praxis aber unter Auflagen genehmigt. In einigen Kreisen Deutschlands wird Vectoring mittlerweile auch von Telekom-Konkurrenten angeboten.

In Kombination mit der Vectoring-Technologie wird auch der Standard G-Fast ausgebaut. Die Technologie ermöglicht die Übertragung von einem Gigabit pro Sekunde über bestehende Kupferkabelinfrastruktur. Die Reichweite von G-Fast ist jedoch auf wenige 100 Meter Reichweite beschränkt, in 100 Meter Entfernung sinkt die maximal erreichbare Geschwindigkeit schon auf maximal 800 Megabit pro Sekunde pro Sekunde. Ein wirklich zukunftsfähiger Ausbau ist durch den Einsatz von Vectoring und G-Fast also nicht möglich. Es handelt sich eher um Brückentechnologien.

Streit um privaten Glasfaserausbau

Immer wieder wird der Telekom vorgeworfen, bei Angeboten an Kommunen für einen flächendeckenden Glasfaserausbau bis ins Haus sehr zurückhaltend zu agieren. Erst wenn sich eine lokale Initiative gründe oder wenn sich alternative Anbieter wie die Deutsche Glasfaser fänden, so Kritiker, werde die Telekom aktiv. Entsprechende Vorwürfe gab es zum Beispiel durch den Landrat im strukturschwachen Landkreis Lüchow-Dannenberg in Niedersachsen.

Das Recht auf einen Internetzugang wurde auf internationaler Ebene erstmals im Jahr 2003 auf dem von den Vereinten Nationen veranstalteten World Summit on the Information Society (WSIS) kodifiziert.

Aufseiten der Zivilgesellschaft fordern deshalb Organisationen wie zum Beispiel der Verein D21 ein verstärktes Engagement der Politik für einen flächendeckenden Ausbau der Glasfasertechnologie. Gemeinsam mit Ministerien und dem Branchenverband Bitkom sowie dem VATM (Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.), dem Deutschen Industrie- und Handelskammertag, dem Verband Deutscher Kabelnetzbetreiber e.V. betreibt der Verein die Deutsche Breitbandinitiative.

International

Die Breitbandkapazitäten sind weltweit sehr ungleich verteilt, auch wenn mittlerweile ein Großteil der Länder, von selbst gewählten Ausnahmen

wie Nordkorea abgesehen, ans Internet angeschlossen ist. In wenigen Ländern wird freies Internet als Grundrecht angesehen, etwa in Estland. Das Recht auf einen Internetzugang wurde auf internationaler Ebene erstmals im Jahr 2003 auf dem von den Vereinten Nationen veranstalteten World Summit on the Information Society (WSIS) kodifiziert. In der Erklärung heißt es, man habe den gemeinsamen Wunsch „eine menschenzentrierte, inklusive und entwicklungsorientierte Informationsgesellschaft auf[zu] bauen, in der jeder Informationen und Wissen kreieren, besuchen, nutzen und weiterverbreiten" könne. Die Prinzipen des WSIS-Gipfels prägen die Internet Governance bis heute: Sie tauchen in ähnlicher Form zum Beispiel im Abschlussdokument des NetMundial-Prozesses auf.

Zu den größeren Akteuren für den Breitbandausbau gehört die Allianz für ein bezahlbares Internet (Alliance for Affordable Internet, A4AI). Finanziert wird die Initiative auch durch Spenden und Zuwendungen von privaten Akteuren, unter anderem von dem Suchmaschinenkonzern Google, von Facebook, dem Netzwerkhersteller Cisco, dem Chiphersteller Intel und dem Omidyar-Netzwerk des Ebay-Gründers Pierre Omidyar. Von staatlicher Seite sind das britische Department for International Development der UN-Frauenorganisation UN Woman involviert.

A4AI setzt sich dafür ein, dass Breitband-Internetanschlüsse für weniger als fünf Prozent des durchschnittlichen Pro-Kopf-Einkommens verfügbar werden. Etwa 40 Prozent der Staaten haben den Zahlen der Initiative zufolge entweder gar keine Breitbandstrategie oder stark veraltete Breitbandziele. Um dieses Ziel zu erreichen, soll unter anderem eine „innovative" Nutzung des Funkspektrums angestrebt werden. Auch der Erfahrungsaustausch soll gestärkt werden. Der weitere Ausbau von Netzwerkinfrastrukturen soll außerdem durch die Nutzung von Universal Service and Access Funds gestärkt werden – einem Instrument, bei dem ein Teil der Umsätze von Telekommunikatonsunternehmen genutzt wird, um eigentlich unrentable Regionen an das Internet anzuschließen.

Der Ausbau der Internetverbindungen schreitet dabei global voran. Vor zehn Jahren noch waren nur 20 Prozent der Weltbevölkerung online, im Jahr 2017 sollen erstmals über 50 Prozent Zugang zum Internet haben. Neben den Vereinten Nationen und den betroffenen Staaten bemühen sich auch Unternehmen und private Vereine um eine bessere Anbindung an das globale Netz. Um eine Internetversorgung in entlegenen Regionen zu ermöglichen, sind Festnetzverbindungen meist keine Option. Verschiedene Anbieter experimentieren deshalb mit alternativen Übertragungstechniken. Facebook setzt mittlerweile auf eine selbst entwickelte Drohne mit dem

Namen Aquila, die mehrere Wochen über einem Gebiet kreisen soll. Der Google-Konzern Alphabet hingegen experimentiert mit seinem Project Loon mit Internetverbindungen, die von Ballons aus bereitgestellt werden.

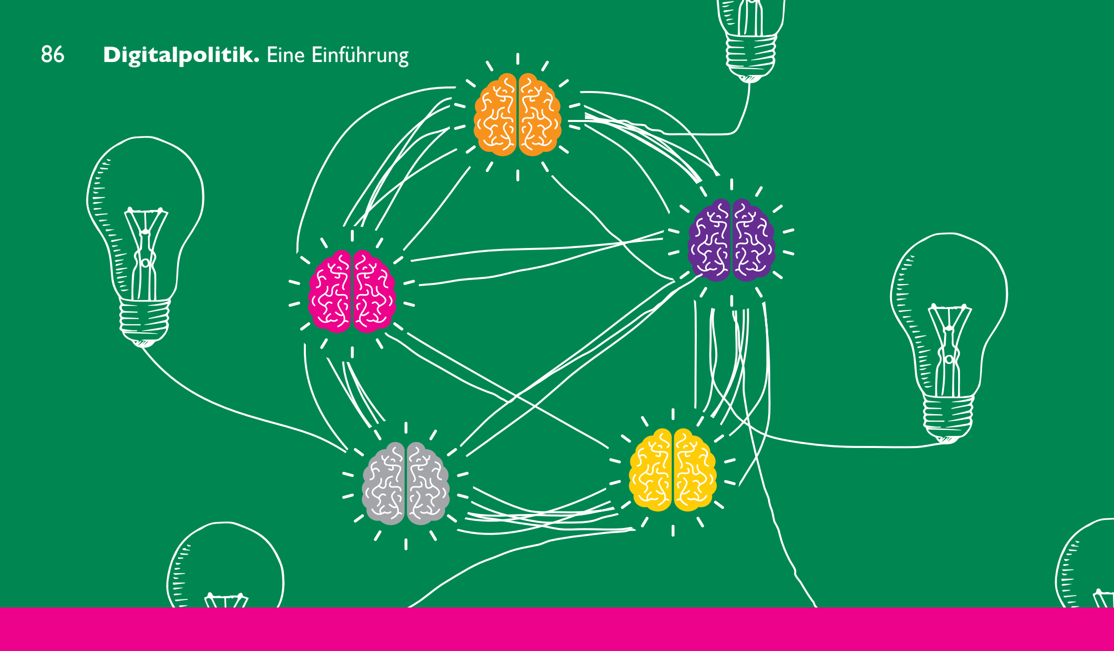
Die von Unternehmen zum Zwecke des Ausbaus von Internetverbindungen eingesetzten Methoden sind allerdings oftmals umstritten. Vor allem in Indien sorgte ein Vorstoß von Facebook-Chef Marc Zuckerberg für Auseinandersetzungen. Zuckerberg will kostenfreien Zugang zu den Produkten seines eigenen Unternehmens und einigen ausgewählten Diensten anbieten, also Facebook selbst, den Facebook Messenger und das Bildnetzwerk Instagram. Neben diesen Diensten gibt es kostenfreien Zugang unter anderem auch zu dem Wissensnetzwerk Wikipedia, der Bing-Suche, verschiedenen Wetterdiensten, und Ask.com. Nicht alle aufgeführten Seiten sind in allen teilnehmenden Ländern verfügbar. Konkurrenzprodukte zu Facebook, insbesondere von Google, sind nicht darunter.

Die ursprünglich unter dem Namen Internet.org gestartete Initiative wurde im Jahr 2015 in Facebook Free Basics umbenannt. In Indien ist das Angebot seit dem Frühjahr 2016 verboten, weil es gegen das Prinzip der Netzneutralität verstoßen soll und Menschen an die Dienste von Facebook bindet, ohne eine Alternative anzubieten. Eine aktive Kooperation zwischen Facebook und Mobilfunkcarriern gibt es vor allem in afrikanischen Ländern, unter anderem Zambia, Tanzania, Malawi, Ghana, Senegal, Bolivien und Angola, außerdem in Indonesien, Guatemala, Kolumbien und Bangladesh. (Der Dienst ist nicht zu verwechseln mit dem Zero-Rating Angebot „Facebook Zero“. Unter diesem Programm bietet Facebook in Zusammenarbeit mit einigen Mobilfunkprovidern einen kostenfreien Zugang zur Facebook-App an, auch wenn Kunden kein Datenvolumen gebucht haben. Weitere Dienste können nicht genutzt werden. In Deutschland gibt es eine entsprechende Partnerschaft mit dem Mobilfunkanbieter E-Plus.)

Ähnliche Partnerschaften für einen begrenzten Zugang zu verschiedenen Diensten haben auch andere Projekte, unter anderem das Online-Lexikon Wikipedia. In verschiedenen Entwicklungs- und Schwellenländern soll das Projekt Wikipedia Zero den kostenfreien Zugang ermöglichen. Auch wenn Wikipedia und die Betreibergesellschaft, die Wikimedia Foundation, kein gewinnorientiertes Unternehmen ist, kritisieren verschiedene Aktivistengruppen Wikipedia Zero als Verletzung des Prinzips der Netzneutralität, weil alternative Wissensprojekte nicht aufgenommen werden und Wikipedia so eine Monopolstellung festigen könne.

Zusammenfassung/Ausblick

Die mittelfristige Realisierung des Breitbandausbaus in Deutschland geht einher mit einer Reihe noch zu lösender politischer Fragen. Dies beginnt mit der Zielsetzung: Welches Niveau von Verbindungsgeschwindigkeiten soll tatsächlich angestrebt werden? Damit verbundene praktische Fragen schließen sich an: Welche Technologie soll beim Ausbau zum Einsatz kommen? Wie soll der Ausbau finanziert werden: Welche Förderinstrumente, welche wirtschaftspolitischen Vorgaben sind zielführend? Im internationalen Kontext stellen sich ähnliche Fragen. Das Spektrum von Übertragungstechnologien, die vor allem für die Versorgung in entlegenen Gebieten zum Einsatz kommen könnten, ist hier noch einmal breiter. Finanzierung und Geschäftsmodelle tangieren, stärker als im nationalen Kontext, grundlegende Fragen der Internetpolitik, wie etwa das Prinzip der Netzneutralität. Viel wird davon abhängen, inwiefern es der Politik auf der einen Seite und Unternehmen und anderen Organisationen, die die Initiative ergreifen, auf der anderen Seite gelingt, gemeinsam Lösungen zu finden. Möglicherweise wird es dazu notwendig sein, Güterabwägungen zwischen dem Ziel einer flächendeckenden Internetverbindung und der Gewährleistung von umfassender Netzneutralität vorzunehmen. ■



Keine Nutzung ohne Vervielfältigung

Durch die fortschreitende Ausweitung seiner Reichweite betrifft das Urheberrecht längst nicht mehr allein die Interessen von Kreativen und Verwertern, sondern nahezu sämtliche digitalen Prozesse.

PAUL KLIMPEL

Für Verbraucher war es noch in den 1980er-Jahren nahezu unmöglich, gegen das Urheberrecht zu verstoßen. Denn bis zur Digitalisierung und dem Aufkommen des Internets kamen damit nur Künstler, Verlage, Plattenlabel, Filmemacher und andere in Berührung, die professionell mit der Verwertung von Kulturerzeugnissen zu tun hatten. Als massenhafte private Kopien von Werken möglich wurden, etwa durch Kassetten- und Videorekorder, entstanden Interessenkonflikte zwischen Verbrauchern und den Beteiligten an den traditionellen Verwertungsketten. Sie wurden durch den Gesetzgeber gelöst, beispielsweise durch eine Abgabe auf Kopiergeräte, die an Urheber und Industrie verteilt wird. Die meisten Menschen merkten davon in ihrem Alltag nichts. Mit der Digitalisierung änderte sich das grundlegend. Das Urheberrecht ist zum Maßstab für jegliche

Nutzung von Inhalten geworden, da jede Nutzung von Inhalten durch digitale Medien technisch bedeutet, dass die Inhalte vervielfältigt werden – und damit urheberrechtlich relevant ist. Auch der Gegenstandsbereich des Urheberrechts erfuhr in vielerlei Hinsicht Erweiterungen. Es beschränkt sich nicht mehr allein auf künstlerisch-kreative Leistungen, sondern umfasst auch technische Prozesse wie beispielsweise Computerprogramme.

Gesellschaftspolitisch verlangt die Ausgestaltung des Urheberrechts immer wieder die Balance zwischen den Interessen von Urhebern, von klassischen Verwertern wie Verlagen und Plattenlabels, von Nutzern wie auch von den neu entstandenen Vermittlern (Intermediären). Vermittler ist, wer an der Speicherung, Verfügbarmachung und Auffindbarkeit von kreativen Leistungen im weitesten Sinne teilhat. Dazu zählen Plattformbetreiber, Web-Hosting- oder Web-Sharing-Dienste, Suchmaschinenanbieter, elektronische Programmführer oder vergleichbare Dienste. Auch Telekommunikationsanbieter sind in diesem Sinne „Vermittler“. Die Abwägung zwischen den Interessen wird erschwert durch die Tendenz, dass vielfach verschiedene Rollen gleichzeitig eingenommen werden. Bekanntestes Beispiel ist der „Prosumer“, eine sich aus den Begriffen Produzent und Konsument zusammengesetzte Wortbildung, die zeigt, dass häufig Konsumenten – und damit Nutzer im klassischen Sinn – gleichzeitig Produzenten neuer Inhalte sind.

Gesellschaftspolitisch verlangt die Ausgestaltung des Urheberrechts immer wieder die Balance zwischen den Interessen von Urhebern, von klassischen Verwertern wie Verlagen und Plattenlabels, von Nutzern wie auch von den neu entstandenen Vermittlern (Intermediären).

Öffentliche Meinungsbildung

Gesellschaftspolitisch hat die Handhabung des Urheberrechts starke Auswirkungen auf die demokratischen Prozesse der Meinungsbildung und des öffentlichen Diskurses. Intermediäre, wie beispielsweise Social-Media-Plattformen, spielen hier heute eine wichtige Rolle. Plattformbetreiber haften zwar nicht für jede Urheberrechtsverletzung derer, die ihre technische Infrastruktur nutzen; sie sind aber verpflichtet, Inhalte zu entfernen, wenn sie von Rechtsverletzungen erfahren. Hier besteht die Gefahr, dass Plattformbetreiber Inhalte selbst dann entfernen, wenn die behauptete Rechtsverletzung fragwürdig ist, um juristisch nicht verantwortlich gemacht werden zu können (siehe die „Takedown Hall of Shame“ der Electronic Frontier Foundation). Diese Eingriffe können zensurähnlichen Charakter haben.

Darüber hinaus hat sich das Urheberrecht zunehmend zu einem Instrument entwickelt, mit dem Akteure die unerwünschte Verbreitung von Informationen bekämpfen. Dies gilt zum Beispiel für behördliche Unterlagen. Statt mit den Regeln von Vertraulichkeit und dem Umgang mit sogenannten Staatsgeheimnissen zu argumentieren (die immer auch gewisse Abwägun-



Die “Takedown Hall of Shame” der Bürgerrechtsorganisation Electronic Frontier Foundation (EFF): eine Sammlung von Fällen, in denen Rechteinhaber Inhalte aus dem Netz entfernen ließen, indem sie angaben, dass dadurch ihre Urheberrechte verletzt worden seien – was aber nach Ansicht der EFF lediglich vorgeschoben wurde, um unliebsame Inhalte aus dem Netz zu löschen.

https://www.eff.org/takedowns

gen zulassen), wird auf den urheberrechtlichen Schutz solcher Unterlagen verwiesen („BGH entscheidet über Urheberrechtsschutz für BMVg-Papiere“, 2017).

Das Urheberrecht ist damit entscheidendes Kriterium dafür, welche Informationen öffentlich zugänglich sind. Davon ist auch der Umgang mit dem kulturellen Erbe betroffen. So sind die kulturellen Zeugnisse des letzten Jahrhunderts weitgehend noch urheberrechtlich geschützt. Es ist jedoch in sehr vielen Fällen unmöglich, die Rechte für deren Nutzung zu klären, also die Zustimmung aller betroffenen Rechteinhaber (Autoren, Verlage, Produktionsfirmen usw.) einzuholen. Viele dieser Werke können daher in der digitalen Welt nicht mehr genutzt werden. Faktisch verschwinden sie somit aus dem öffentlichen Bewusstsein. Besser zugänglich dagegen sind Zeugnisse aus US-amerikanischen Quellen, da die dortige Rechtslage die Massendigitalisierung des kulturellen Erbes weitergehender erlaubt als in Europa. Rechtsexperten und Vertreter deutscher Kulturinstitutionen befürchten, dass dieses Ungleichgewicht eine „erhebliche Verzerrung unseres Geschichtsbildes“ zur Folge haben könnte („Hamburger Note“).

Technische und rechtliche Tangenten

Auswirkungen hat das Urheberrecht auch auf das Design technischer Systeme. Ein Beispiel hierfür ist das Geoblocking, also die Beschränkung des Zugangs zu Medieninhalten, abhängig davon, wo ein Nutzer sich aufhält. Geoblocking steht der Entwicklung einer gemeinsamen europäischen Öffentlichkeit entgegen. Ein anderes Beispiel ist der politisch diskutierte verpflichtende Einsatz sogenannter Upload-Filter. Wer mit großen Mengen von Daten befasst ist, soll nach Überlegungen der EU-Kommission verpflichtet werden, technische Filter zu installieren, die urheberrechtlich geschütztes Material erkennen und aussortieren würden. Dieses an der „Content ID“ bei YouTube orientierte Verfahren soll Urheberrechtsverstöße verhindern. Kritiker bemängeln: Von Upload-Filtern wären auch solche Materialien betroffen, die zwar urheberrechtlich geschützt sind, deren

Verwendung im konkreten Fall aber legal ist – beispielsweise als Zitat. Mit einer Pflicht zu Upload-Filtern würden große Projekte mit freien Inhalten, wie die Wikipedia Commons, unmöglich gemacht.

Wichtig ist, dass mit dem Übergang von analogen zu digitalen Inhalten sich die Rechtsposition der Erwerber von Medien erheblich verschlechtert hat. Während der Käufer von Büchern Sacheigentum erwarb und dieses auch problemlos weiterveräußern oder vererben konnte, ohne jemanden um Erlaubnis zu fragen, ist das bei E-Books nicht mehr möglich. Endverbraucher solcher ‚unkörperlichen' Werke erwerben lediglich Nutzungslizenzen, die vielfältigen Einschränkungen unterliegen. Der sogenannte „Erschöpfungsgrundsatz", nach dem sich Schutzrechte „verbrauchen", sobald der geschützte Gegenstand rechtmäßig in den Verkehr gebracht wurde, gilt bei digitalen Medien nicht.

Derzeit wird auf europäischer Ebene diskutiert, ein Leistungsschutzrecht für Presseverlage einzuführen. Der Intention nach soll dieses Recht dazu führen, dass Verlage finanziell davon profitieren können, wenn Google und andere Suchmaschinen auf von Verlagen bereitgestellte Inhalte verweisen und wenn dabei kleine Teile dieser Inhalte („Snippets") angezeigt werden, die sonst nicht urheberrechtlich geschützt sind. In Deutschland, wo ein solches Leistungsschutzrecht 2013 eingeführt wurde, ist es indes noch zu keinen Zahlungen von Google gekommen. Es wurde sogar die Marktkonzentration großer Anbieter gestärkt, da diese mit erheblichen Ressourcen die neuen gesetzlichen Vorgaben parieren konnten, während kleinere Anbieter und Start-ups durch die Pflicht zur Lizenzierung von Snippets in Bedrängnis gerieten (siehe zum Beispiel die Berichterstattung in „Die Zeit" zum Fall uberMetrics).

Creative-Commons-Lizenzen wurden entwickelt, um das Schutzniveau kontrolliert zurückzufahren und eine weitergehende Nutzung von geschütztem Material zu ermöglichen.

Neben den rechtlichen und technischen Tangenten des Urheberrechts spielt in der Debatte zum Schutz von Kreativleistungen im digitalen Umfeld vor allem auch die Konzeption der Creative Commons als ein alternatives Urheberrechte-Regime eine wichtige Rolle. Creative-Commons-Lizenzen wurden entwickelt, um das Schutzniveau kontrolliert zurückzufahren und eine weitergehende Nutzung von geschütztem Material zu ermöglichen. Creative-Commons-Lizenzen räumen dem Urheber oder Rechteinhaber außerdem eine weitgehende Gestaltungsmöglichkeit in der Definition von Nutzungsrechten ein. Creative-Commons-Lizenzen haben seit ihrer Einführung im Jahr 2001 eine enorme Verbreitung erfahren – sowohl in Bildung und Wissenschaft als auch bei kulturellen Institutionen und auf kommerziellen Plattformen. Auch die weltweit größte Plattform freier Informationen, die Wikipedia, ist nur möglich, weil hier freie Lizenzen zum Einsatz kommen.

Internationale Rahmenbedingungen im Überblick

Die 1887 geschlossene und seitdem mehrfach revidierte Berner Übereinkunft, einer der ältesten internationalen Verträge überhaupt, führt heute dazu, dass urheberrechtlicher Schutz nahezu überall auf der Welt gilt. Die Übereinkunft sieht vor, dass jeder Vertragsstaat den Schutz an Werken von Bürgern anderer Vertragspartner genauso anerkennt wie den Schutz von Werken der eigenen Bürger. Trotz der Berner Übereinkunft und trotz eines gewissen Grades an Harmonisierung innerhalb der EU – insbesondere durch die sogenannte InfoSoc-Richtlinie (s.u.) – unterscheidet sich die Praxis urheberrechtlichen Schutzes jedoch erheblich in den unterschiedlichen nationalen Rechtsordnungen. Die auf dem Case Law beruhenden Rechtsordnungen und insbesondere das US-amerikanische Recht mit seiner Doktrin des „Fair Use“ erlauben eine sehr viel flexiblere Reaktion auf neue technische Entwicklungen. Die hat zur Folge, dass in den USA Massendigitalisierungsprogramme wie zum Beispiel Google Books oder das Internet Archiv möglich sind, die in Europa rechtlich unzulässig wären. Die Rechtslage hat auch zur Folge, dass urheberrechtlich geschützte Inhalte insgesamt mehr genutzt werden.

Die 1887 geschlossene und seitdem mehrfach revidierte Berner Übereinkunft, einer der ältesten internationalen Verträge überhaupt, führt heute dazu, dass urheberrechtlicher Schutz nahezu überall auf der Welt gilt.

Aber auch innerhalb von Europa unterscheidet sich die Praxis gravierend. In den skandinavischen Staaten gibt es eine lange Tradition kollektiver Lizenzen und damit auch in der digitalen Welt die Praxis, urheberrechtliche Fragestellungen, die nicht die – meist nur kurz dauernde – Primärverwertung von Werken betrifft, über Kollektivlizenzen zu lösen. In anderen europäischen Ländern hingegen findet die Nutzung urheberrechtlich geschützter Werke kaum noch statt, wenn diese ihren Verwertungszyklus hinter sich haben und die Kosten für die Klärung von Rechten unverhältnismäßig hoch wären.

Die grundlegende Weichenstellung für die rechtlichen Rahmenbedingungen im Netz erfolgte in Europa mit der sogenannten InfoSoc-Richtlinie zur Harmonisierung des Urheberrechts und verwandter Schutzrechte im Jahr 2001. Mit der Richtlinie wurde der Urheberrechtsvertrag der Berner Übereinkunft durch die Europäische Gemeinschaft umgesetzt. Sie ist bis heute grundlegend für die Europäische Union. Die der InfoSoc-Richtlinie zugrunde liegenden politischen Abstimmungsprozesse fanden Ende der 90er-Jahre statt – zu einer Zeit also, als das Internet noch nicht den Alltag weiter Teile der Bevölkerung beherrschte. Sowohl bei der Formulierung der Richtlinie, wie auch bei der späteren Umsetzung in deutsches Recht kam es zu ersten scharfen Auseinandersetzungen, insbesondere in Hinblick auf das Recht auf Privatkopie.

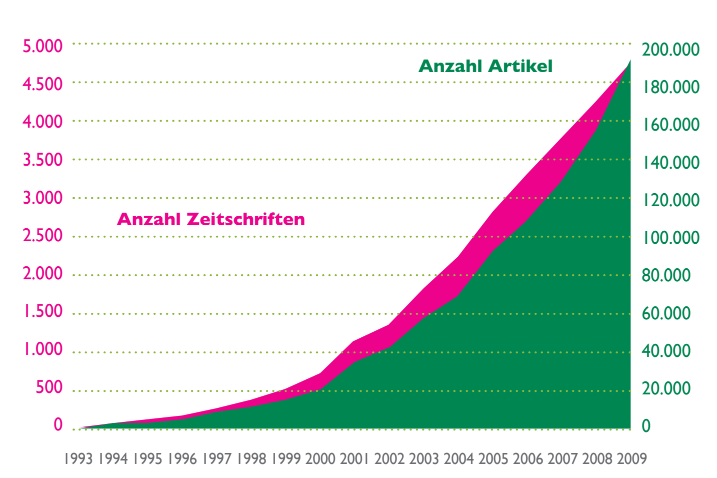
Der Kampf um die „Privatkopie“

Das Recht auf die Privatkopie wurde von der InfoSoc-Richtlinie zwar grundsätzlich bestätigt. Zugleich jedoch wurde es ausgehöhlt: Mit der neuen Richtlinie wurde jegliche Umgehung von Kopierschutz strafbar. Somit wurde Rechteinhabern die Möglichkeit an die Hand gegeben, mittels Kopierschutz (DRM, Digital Rights Management) zu verhindern, dass Privatkopien überhaupt erst legal erzeugt werden konnten. Grund für die restriktive Gesetzgebung war die Befürchtung, dass aufgrund von nicht erlaubten Nutzungen die bisherigen, auf Kopienkontrolle beruhenden Geschäftsmodelle insbesondere der Unterhaltungsindustrie gefährdet würden. Ungeachtet der Gesetzgebung hat inzwischen gerade die Musikindustrie, deren Interessen diese Regelung dienen sollte, auf den Einsatz dieser Technologie weitgehend verzichtet, weil sie von den Verbrauchern nicht angenommen wurde.

Die Umsetzung der InfoSoc-Richtline in deutsches Recht erfolgte in zwei Schritten: „erster Korb“ und „zweiter Korb“. Im ersten Korb von 2003 wurde insbesondere das Recht der öffentlichen Zugänglichmachung (das ‚Online-Stellen‘) als eigene Nutzungsart benannt. Im zweiten Korb, dessen Regelungen 2008 in Kraft traten, wurde das vormals geltende Verbot der Übertragung unbekannter Nutzungsarten aufgehoben. Rechteverwerter können seitdem mit Erbringern kreativer Leistungen (und mit anderen Rechteinhabern) pauschale Verträge abschließen, die die Nutzung der entsprechenden Werke auf innovative Weisen erlauben, die zum Zeitpunkt des Vertragsabschlusses noch unbekannt sind. Zudem ermöglichte der zweite Korb die Nutzung von digitalen Kopien an Terminals von Bibliotheken und Archiven und enthielt eine sehr komplizierte Regelung für bestimmte Nutzungen von urheberrechtlich geschützten Werken in Bildung und Wissenschaft. Eine vielfach geforderte Bagatellgrenze für Urheberrechtsverletzungen wurde hingegen nicht ins Gesetz aufgenommen. Jede Nutzung eines urheberrechtlich geschützten Werkes ohne die Erlaubnis des Rechteinhabers ist in Deutschland somit strafbar (§ 106 UrhG).

Verbreitung von Creative-Commons-Lizenzen/Anteil CC-Lizenzen: Entwicklung 1993-2009

https://en.wikipedia.org/wiki/Open_access



In der Folgezeit kam es zu vereinzelten Änderungen. Insbesondere wurde die Europäische Richtlinie zur Nutzung von verwaisten Werken umgesetzt und ein Leistungsschutzrecht für Presseverlage geschaffen (s.o.). Keinen Erfolg hatte der vor allem durch die Grünen in die politische Diskussion eingebrachte Vorschlag einer „Kulturflatrate“ – einer Pauschalabgabe für die Nutzung von urheberrechtliche geschützten Inhalten im Internet, mit der die Interessen von Nutzern und Rechteinhabern ausgeglichen werden sollten.

Noch in der Diskussion ist die Einführung einer allgemeinen Bildungs- und Wissenschaftsschranke. Diese würde zum Beispiel wissenschaftlichen Bibliotheken den Versand elektronischer Kopien erlauben, rechtliche Klarheit in Bezug auf die Online-Bereitstellung von Lehrmaterialien schaffen oder die automatisierte Auswertung ganzer Editionen zum Zwecke der wissenschaftlichen Textanalyse erleichtern. Die Einführung einer Bildungs- und Wissenschaftsschranke wurde bereits in verschiedenen Koalitionsverträgen als Ziel benannt und auch durch die für Bildung und Wissenschaft zuständigen Länder im Bundesrat verschiedentlich angemahnt. Anfang 2017 veröffentlichte das Bundesministerium der Justiz und für Verbraucherschutz den Entwurf eines „Gesetzes zur Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft“, das die bisherigen Regelungen neu ordnet und verständlich macht. Außerdem schreibt der Entwurf grundsätzlich das Prinzip der pauschalisierten Vergütung für bestimmte erlaubte Nutzungen fest. Um die Umsetzung dieses Entwurfs wird derzeit erbittert gerungen. Während Verlage eine Verschlechterung ihrer Position befürchten, wird der Vorschlag durch Wissenschaft und Bibliotheken grundsätzlich begrüßt, auch wenn er einigen nicht weit genug geht.

Akteure

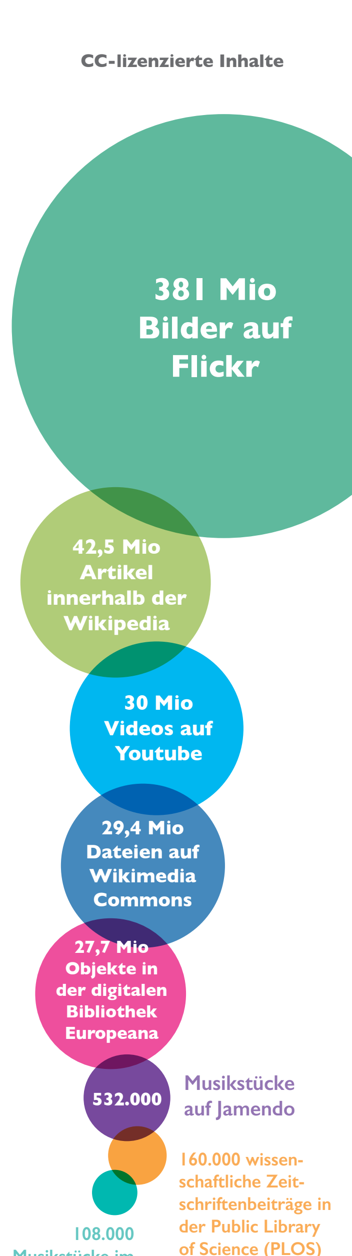
In der Urheberrechtsgesetzgebung versuchen unterschiedliche Interessengruppen Einfluss auf die politische Entscheidungsfindung zu nehmen. Dabei sind die Interessen von Urhebern, Verwertern, Nutzern wie auch den neu entstandenen Vermittlern unterschiedlich und vielfach gegensätzlich. Urheber und Verwerter beispielsweise bilden in Bezug auf das Urheberrecht mitnichten notwendig eine Interessengemeinschaft. Dies bezeugt allein schon das Urhebervertragsrecht, in dem Konflikte zwischen den beiden Gruppen benannt und geregelt werden. Im politischen Diskurs werden dennoch oft die gemeinsamen Interessen von Urhebern und Verwertern betont, zum Beispiel durch den Börsenverein des Deutschen Buchhandels, die verschiedenen Dachverbände von Film- und Musikindustrie und die zu diesem Zweck eigens gegründete „Deutsche Content Allianz“ sowie den Deutschen Kulturrat.

Veränderungen und Reformen werden meist nur für einen bestimmten Bereich und von spezifischen Interessengruppen gefordert. Dazu gehört insbesondere die Wissenschaft, deren entschiedenster Vertreter das „Aktionsbündnis Urheberrecht für Bildung und Wissenschaft" ist. Der Legalisierung von Remixes und Mashups, die durch Internet und Digitaltechnologie ermöglicht wurden, hat sich eine Initiative verschrieben, die ein „Recht auf Remix" fordert. IGEL, die Initiative gegen ein Leistungsschutzrecht für Presseverleger, hat sich ausschließlich dem Kampf gegen das Leistungsschutzrecht verschrieben. Auch das Aufkommen und zwischenzeitliche Erstarken der „Piratenpartei" war ein Ausdruck des Unbehagens am als restriktiv empfundenen Urheberrecht.

Weitere wichtige Vertreter im urheberrechtlichen Diskurs sind Initiativen, die sich freiem Wissen verschrieben haben, wie die Open Knowledge Foundation oder Wikimedia Deutschland. Vonseiten der Industrie gehen parallele Bestrebungen von Unternehmen aus, deren Geschäftsmodell als Vermittler nicht auf der Restriktion des Umgangs mit Inhalten beruht, sondern im Gegenteil darauf, dass möglichst viele Inhalte genutzt werden und damit wertvolle Informationen über die jeweiligen Nutzer generiert werden können. Dies gilt insbesondere für Google, ist aber nicht auf die Firma beschränkt. Die meisten innovativen Unternehmen der IT hadern mit den als zu restriktiv empfundenen urheberrechtlichen Rahmenbedingungen.

Konklusion

Mit der Digitalisierung und dem Aufkommen des Internets hat das Urheberrecht zentrale Bedeutung für die demokratischen Prozesse der Meinungsbildung und des öffentlichen Diskurses erlangt. Grund dafür ist, dass beim Einsatz digitaler Technologie jede Nutzung automatisch auch eine urheberrechtlich relevante Vervielfältigung ist. Durch die fortschreitende Ausweitung seiner Reichweite betrifft das Urheberrecht längst nicht mehr allein die Interessen von Kreativen und Verwertern. Deshalb erscheint es besonders wichtig, die vielfältigen (und oft gar nicht intendierten) gesellschaftlichen Auswirkungen des Urheberrechts im Blick zu behalten. ■



Quelle: Creative Commons: *2016 State of the Commons Report*

Herausgeber

Lorena Jaume-Palasí forscht zu Rechtsphilosophie und politischer Philosophie im digitalen Zeitalter und fokussiert sich auf die zeitgenössische Vorstellung und die Dynamiken digitaler Öffentlichkeit und Privatheit, insbesondere auf ethische Konflikte und Normen. Unter anderem beriet sie als eine von acht externen Experten Googles Advisory Council zum Thema „Recht auf Vergessen". Sie ist Mitgründerin von AlgorithmWatch und der Dynamic Coalition on Publicness des Internet Governance Forums der Vereinten Nationen (UN IGF) und leitet das Sekretariat des deutschen Internet Governance Forums (IGF-D). Lorena Jaume-Palasí ist Mitglied im Expertenbeirat der internationalen Initiative „Code Red" gegen Massenüberwachung. Derzeit ist sie Bucerius-Fellow der ZEIT-Stiftung.

Dr. Julia Pohle ist Kommunikationswissenschaftlerin und Mitarbeiterin in der Projektgruppe „Politikfeld Internet" am Wissenschaftszentrum Berlin für Sozialforschung (WZB). In ihren international veröffentlichten Forschungsarbeiten beschäftigt sie sich mit Internetregulierung, Internet Governance und globalen Strukturen der Kommunikationspolitik. Sie ist Mitglied des Lenkungskreises des Internet Governance Forums Deutschland (IGF-D) und Vize-Vorsitzende der Sektion für Kommunikationspolitik und Technology der International Association for Media and Communication Research (IAMCR). 2014/15 war sie Fellow des Global Governance Futures Programm (GGF) der Robert Bosch Stiftung und zwischen 2013 und 2016 Mitglied des Steering Committees des Global Internet Governance Academic Networks (GigaNet). Von 2007 bis 2010 arbeitete Julia Pohle im UNESCO-Sekretariat in Paris.

Matthias Spielkamp ist Mitgründer von AlgorithmWatch und Gründungsmitglied und Herausgeber von iRights.info (Grimme Online Award). Er hatte Lehraufträge an verschiedenen deutschen Hochschulen und war Sachverständiger des Bundestags zu künstlicher Intelligenz und Robotik, Geheimdienstkontrolle, Online-Journalismus und Urheberrecht. Derzeit ist er Bucerius-Fellow der ZEIT-Stiftung; 2015/16 war er Fellow der Stiftung Mercator und Gastwissenschaftler am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG). Spielkamp ist Mitglied im Vorstand bei Reporter ohne Grenzen Deutschland, außerdem im Beirat des Whistleblower-Netzwerks und des Studiengangs Politik & Public Affairs der Quadriga Hochschule Berlin. Im Lenkungskreis des deutschen Internet Governance Forums (IGF-D) ist er Co-Chair für die Gruppen Wissenschaft und Zivilgesellschaft. Bücher: *Guidebook Internet Governance* (Hrsg. 2016), *Groundbreaking Journalism* (Hrsg. 2014); *Arbeit 2.0,* 2009 (mit V. Djordjevic et al.); *Urheberrecht im Alltag,* 2008 (mit V. Djordjevic et al.); *Schreiben fürs Web,* 2003 (mit M. Wieland).

Autoren

Jürgen Geuter arbeitet als Projektleiter und Consultant bei der Boom Software GmbH. In dieser Aufgabe entwickelt und betreut er Industrie-4.0-Projekte für Kunden aus diversen Industriesparten mit besonderem Fokus auf die Verknüpfung von Produktion, Instandhaltung und Maschinendatenauswertungen.

Hauke Gierow schreibt für Golem.de seit September 2015 über IT-Security, Datenschutz und Urheberrecht. Die koreanische Starcraft-Liga interessiert ihn mehr als die Fußball-Bundesliga. Bevor er in den Journalismus wechselte, arbeitete er für Reporter ohne Grenzen, das Mercator Institut für China-Studien (Merics) und die Open Knowledge Foundation. Er ist Fellow im Programm Transatlantic Digital Debates. Sein Studium der Politikwissenschaften und Sinologie absolvierte er in Trier und Xiamen.

Friedhelm Greis ist seit Juni 2013 Redakteur für Netzpolitik bei Golem.de. Der gelernte Energieanlagenelektroniker studierte Elektrotechnik, Theologie, Spanisch, Philosophie und Journalistik in Trier, Mainz und Bolivien. Er arbeitete bei der Netzeitung, als Journalist und freier Autor in New York und Berlin und als Herausgeber und Redakteur bei der Nachrichtenagentur ddp/dapd. Er betreibt das Tucholsky-Blog Sudelblog.de und schreibt für die Wikipedia.

Dr. Ralf Grötker ist wissenschaftlicher Redakteur und Mitglied des Journalistenbüros Schnittstelle. Digitalpolitik und Technikfolgendiskussion gehören zu seinen Arbeitsschwerpunkten. Im Jahr 2003 erschien der von ihm herausgegebene Sammelband *Privat! Kontrollierte Freiheit in einer vernetzten Welt.* 2015 verfasste er für den Thinktank Netopia die Studie *The Citizens' Internet. The many threats to neutrality.* Grötker wurde von der Freien Universität Berlin im Fach Philosophie promoviert; zuvor studierte er an den Universitäten Bremen, Paris und Köln.

Joerg Heidrich ist seit 2001 als Justiziar und Datenschutzbeauftragter des Heise Zeitschriften Verlags sowie als Rechtsanwalt in Hannover tätig. Er ist Fachanwalt für IT-Recht und Sachverständiger für IT-Produkte. Nach dem Studium der Rechtswissenschaften in Köln und Concord, NH (USA), beschäftigt er sich seit 1997 mit den Problemen des Internet- und Medienrechts. Heidrich ist Autor zahlreicher Fachbeiträge und Referent zu rechtlichen Aspekten der neuen Medien und des Urheberrechts.

Dr. Matthias C. Kettemann, Jahrgang 1983, studierte Rechtswissenschaften in Graz und Genf und war Fulbright- und Boas-Scholar an der Harvard Law School (LL.M. 2010). 2012 promovierte er an Karl-Franzens-Universität Graz mit einer Arbeit zur Zukunft des Individuums im Völkerrecht. 2006 bis 2013 war er Universitätsassistent und Lektor am Institut für Völkerrecht und Internationale Beziehungen der Universität Graz. Seit Oktober 2013 forscht er als Post-Doc Fellow am Exzellenzcluster Normative Ordnungen der Goethe-Universität Frankfurt am Main, wo er sich zur normativen Ordnung des Internets habilitiert. Er ist Co-Chair der Internet Rights & Principles Coalition, hat für den Europarat, das Europäische Parliament und das Internet&Society Co:llaboratory geforscht und publiziert regelmäßig zu Rechtsfragen des Internets. 2013 erschien von ihm *The Future of Individuals in International Law* (Utrecht) und als (Mit-)Herausgeber *European Yearbook on Human Rights 2013* (Wien), *Grenzen im Völkerrecht* (Wien) und *Netzpolitik in Österreich. Internet. Macht. Menschenrechte* (Wien).

Dr. Paul Klimpel, RA, ist Initiator und Leiter der jährlich stattfindenden internationalen Konferenz „Zugang gestalten! Mehr Verantwortung für das kulturelle Erbe". Von 2006 bis 2011 war er Verwaltungsdirektor der Stiftung Deutsche Kinemathek. In dieser Funktion war er auch Geschäftsführer des Netzwerks Mediatheken und engagierte sich für eine Verbesserung der rechtlichen Rahmenbedingungen von Museen und Archiven, insbesondere des Urheberrechts. Er hat Jura und Philosophie in Bonn, München und Berlin studiert.

Martin Schallbruch studierte Informatik an der TU Berlin sowie Rechtswissenschaft und Soziologie. 1998 begann er als persönlicher Referent von Staatssekretärin Brigitte Zypries im Bundesinnenministerium und stieg dort 2002 zum IT-Direktor des Ministeriums auf. Seine Verantwortung umfasste neben Sicherheitsfragen auch den IT-Einsatz der öffentlichen Verwaltung. 2014 wurde Martin Schallbruch Abteilungsleiter für Informationstechnik, Digitale Gesellschaft und Cybersicherheit. 2016 wechselte er vom Innenministerium an die European School for Management and Technology (ESMT) in Berlin – als Senior Researcher für Cyber Innovation and Cyber Regulation sowie Deputy Director of the Digital Society Institute. Bereits seit 2011 ist Martin Schallbruch Lehrbeauftragter am Karlsruher Institut für Technologie (KIT) und gibt dort regelmäßige Seminare zum Thema „IT-Sicherheit und Recht".

Isabel Skierka forscht am Digital Society Institute (DSI) der ESMT Berlin zu Cybersicherheit und Digitalpolitik. Sie ist non-resident Fellow am Global Public Policy Institute (GPPi) in Berlin und Co-Chair für Nachwuchs im Beirat des Internet Governance Forum Deutschland (IGF-D). Bevor sie 2016 zum DSI kam, arbeitete sie beim GPPi, bei der Nato und bei der EU Kommission zu sicherheits- und digitalpolitischen Themen.

Impressum

Herausgeber: Lorena Jaume-Palasí, Julia Pohle, Matthias Spielkamp
office@irights.international

Eine Publikation des Wikimedia Deutschland e.V. und iRights.international,
mit Unterstützung von ICANN

Redaktion: Ralf Grötker

Korrektorat: Jörg Garbers

Gestaltung: Beate Autering, Tiger Stangl | beworx

Druck: PinguinDruck

Wir empfehlen, bei Zitaten folgende bibliografische Angaben zu machen:
Lorena Jaume-Palasí, Julia Pohle, Matthias Spielkamp (Hg.), *Digitalpolitik. Eine Einführung,* Berlin: Wikimedia Deutschland e.V. und iRights.international, 2017

Partner

Wikimedia Deutschland teilt die Vision der gesamten Wikimedia-Bewegung – eine Welt, in der das gesammelte Wissen der Menschheit jeder Person frei zugänglich ist. Im Mittelpunkt der hauptamtlichen Arbeit stehen dabei die vier Felder ehrenamtliche Communitys, Institutionen aus Bildung, Wissenschaft und Kultur, gesellschaftliche wie politische Rahmenbedingungen sowie die Potenziale freier Software. Gemeinsam mit den weiteren Initiatoren des vorliegenden Readers wollen wir das Wissen über die internationale Netzpolitik vertiefen helfen und darauf hinwirken, dass sich wieder mehr Menschen aus dem deutschsprachigen Raum in die Prozesse der Internet Governance einbringen. Das weltweite Netz der Netze entwickelt sich nach wie vor rasant weiter und es gilt, diese Entwicklung im Sinne des Freien Wissens und der Teilhabe aller zu gestalten. http://wikimedia.de

ICANN tritt für ein stabiles, sicheres und einheitliches globales Internet ein. Um jemanden im Internet zu erreichen, muss man eine Adresse in einen Computer oder ein anderes Gerät eingeben – einen Namen oder eine Nummer. Diese Adresse muss einzigartig sein. Nur so können Computer wissen, wie sie einander finden können. ICANN hilft bei der Koordinierung und Unterstützung von einzigartigen Identifikatoren auf der ganzen Welt. ICANN wurde 1998 von einer Gemeinschaft von Akteuren aus der ganzen Welt als nicht profitorientiertes, gemeinnütziges Unternehmen gegründet. https://icann.org

iRights.international ist eine Nichtregierungsorganisation mit Sitz in Berlin. Gemeinsam mit der öffentlichen Hand, zivilgesellschaftlichen Organisationen und Unternehmen entwickeln wir Forschungsprojekte, Lösungskonzepte und Publikationen zu Fragen der Digitalpolitik und Internet Governance. Unser Leitbild: Die Möglichkeiten der Digitalisierung zu nutzen, um Demokratie und Gemeinwohl zu stärken. Unser Ansatz: Wir unterstützen mit unserer Expertise die kooperative Entwicklung praktikabler Lösungen. http://iRights.international





